

EXPLICIT MOTIVIC CHABAUTY-KIM THEORY III: TOWARDS THE POLYLOGARITHMIC QUOTIENT OVER GENERAL NUMBER FIELDS

ISHAI DAN-COHEN

ABSTRACT. Over the past twelve years or so, Minhyong Kim has developed a framework for making effective use of the fundamental group to bound (or even compute) integral points on hyperbolic curves. This is the third installment in a series whose goal is to realize the potential effectivity of Kim’s approach in the case of the thrice punctured line. As envisioned in [DCW2], we construct an algorithm whose output upon halting is provably the set of integral points, and whose halting would follow from conjectures. Our results go a long way towards achieving our goals over the rationals, while broaching the topic of higher number fields.

1. INTRODUCTION

1.1. This is the third installment in a series [DCW1, DCW2] devoted to what I wish to call *explicit motivic Chabauty-Kim theory*. ‘Chabauty-Kim theory’ refers to a framework developed by Minhyong Kim for making effective use of the fundamental group to bound, or conjecturally compute, integral solutions to hyperbolic equations. ‘Motivic’ refers to the fact that while Kim’s construction, in its original formulation, is p -adic étale, our methods are motivic. This approach, as I hope to convince the reader, is quite powerful. (Indeed, it is currently the only approach which uses Kim’s methods to produce an actual algorithm.) It does, however, limit us to working with curves of *mixed Artin-Tate type*, that is, to the projective line, with possibly interesting punctures (at least in the near-term). So the adjective ‘motivic’ implies a fairly specific context. While this context may seem narrow from a geometric point of view, it is quite broad from an arithmetic point of view, leading and relating to various interesting questions and conjectures.

‘Explicit’ refers to the fact that here our emphasis is on algorithms. *Explicit* Chabauty-Kim theory, as I see it, is somewhat orthogonal to Chabauty-Kim theory proper. *Chabauty-Kim theory* is hopefully, at least in part, about attempting to prove Kim’s conjecture [BDCKW], or at least about formulating and studying a range of related conjectures. By contrast, *Explicit* Chabauty-Kim theory is about making the theory *explicit*. In particular, in the explicit theory, we allow ourselves to assume conjectures left and right, so long as those affect the halting, and not the construction, of the hoped-for algorithms.

In this installment, we continue our study of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$. We obtain an algorithm for computing the *polylogarithmic Chabauty-Kim loci* (see below) over number fields which obey a weak technical condition. We also obtain an algorithmic solution to the unit equation over totally real fields obeying the same condition. Specializing to the case of the rationals, we obtain the algorithm envisioned in Dan-Cohen–Wewers [DCW2].

Date: June 14, 2016.

This work was supported by Priority Program 1489 of the Deutsche Forschungsgemeinschaft: *Experimental and algorithmic methods in algebra, geometry, and number theory*.

1.2. We now state our main application in more detail. Let $X = \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Below, we construct an algorithm which takes as input an integer scheme Z (by which we mean an open subscheme of $\text{Spec } \mathcal{O}_K$ for K a number field), and outputs a subset of $X(Z)$.

Theorem 1.2.1. Let Z be a totally real integer scheme. If our algorithm halts for the input Z , then its output is equal to the set $X(Z)$ of integral points of X over Z .

We also state / recall four conjectures: *Zagier's conjecture*, *Goncharov exhaustion (with weak control over ramification)*, the *p-adic period conjecture*, and *convergence of Chabauty-Kim loci for the polylogarithmic quotient*. Finally, we state our technical condition, which we call *Hasse principle for finite cohomology*. We say that K obeys *Kim vs. Hasse* if convergence occurs *before* the Hasse principle fails (see below for details). The following proposition motivates the theorem above.

Proposition 1.2.2. Let Z be a totally real integer scheme with fraction field K .

- (1) Assume Zagier's conjecture, Goncharov exhaustion, the p-adic period conjecture, and convergence of Chabauty-Kim loci for the polylogarithmic quotient hold for Z . Assume K obeys Kim vs. Hasse. Then our algorithm halts for Z .
- (2) Suppose Z is contained in $\text{Spec } \mathbb{Z}$. Assume Goncharov exhaustion, the p-adic period conjecture, and convergence of Chabauty-Kim loci for the polylogarithmic quotient hold for Z . Then our algorithm halts for Z .

We refer to Theorem 1.2.1 and Proposition 1.2.2, taken together, as the “point-counting theorem”; see Theorem 6.2.1 for a more precise statement.

1.3. We now give a brief indication of our main result, from which the point-counting theorem follows as a corollary; precise statements, as well as more background, appear in section 2 below. For this purpose, fix a prime $\mathfrak{p} \in Z$ which we assume to be totally split and recall that there is a commutative diagram like so.

$$\begin{array}{ccc} X(Z) & \longrightarrow & X(Z_{\mathfrak{p}}) \\ \kappa \downarrow & & \downarrow \kappa_{\mathfrak{p}} \\ \mathbb{Q}_p \otimes H^1(U_{\geq -n}^{\text{PL}}) & \xrightarrow{\text{reg}_{\mathfrak{p}}} & H^1(U_{\geq -n}^{\text{PL}, F\phi}). \end{array}$$

Here $Z_{\mathfrak{p}}$ denotes the complete local scheme of Z at \mathfrak{p} , isomorphic to $\text{Spec } \mathbb{Z}_{\mathfrak{p}}$, $U_{\geq -n}^{\text{PL}}$ denotes the level- n quotient of the polylogarithmic quotient of the unipotent fundamental group of X at the tangential base point $\vec{1}_0$, a certain quotient of a unipotent, motivic version of the fundamental group. The cohomology variety $H^1(U_{\geq -n}^{\text{PL}})$ appearing below left is a certain \mathbb{Q} -variety parametrizing torsors for $U_{\geq -n}^{\text{PL}}$. The vertical map κ sends an integral point x to the torsor of homotopy classes of paths

$$\vec{1}_0 \rightarrow x.$$

The cohomology variety appearing in the lower-right is a certain p -adic variant of the one to its left, based, as the notation suggests, on the theory of filtered ϕ modules. In terms of this diagram, we define

$$X(Z_{\mathfrak{p}})_n := \kappa_{\mathfrak{p}}^{-1}(\text{Im reg}_{\mathfrak{p}}).$$

We construct an algorithm for computing the locus $X(Z_{\mathfrak{p}})_n$ to given p -adic precision.

Theorem 1.3.1 (c.f. Theorem 2.4.1 below). Let Z be a totally real integer scheme, \mathfrak{p} a totally split prime, n a natural number, and $\epsilon > 0$. If our algorithm halts for these inputs, then the functions $\tilde{F}_i^{\mathfrak{p}}$ which the algorithm returns as output take values less than ϵ on $X(Z_{\mathfrak{p}})_n$.

1.4. The main problem of explicit Chabauty-Kim theory is to render the map $\text{reg}_{\mathfrak{p}}$ computationally accessible; in the case at hand, we proceed as follows. Let $U(Z)$ denote the unipotent part of the fundamental group of the category of mixed Tate motives over Z . If $Z^o \subset Z$ is an open subscheme, there's an associated surjection

$$U(Z^o) \twoheadrightarrow U(Z).$$

As part of the algorithm, we search for a Z^o such that $U(Z^o)$ admits a *nice* set of coordinates. More will be said about the role played by Z^o below; for now, let us fix Z^o arbitrarily. A theory of p -adic iterated integration due to Coleman and Besser gives rise to a point

$$I_{BC} : \text{Spec } \mathbb{Q}_p \rightarrow U(Z^o).$$

Our construction revolves around the following diagram.

$$\begin{array}{ccc} \text{Spec } \mathbb{Q}_p \times H^1(U_{\geq -n}^{\text{PL}}) & \xrightarrow{\text{reg}_{\mathfrak{p}}} & H^1(U_{\geq -n}^{\text{PL}, F\phi}) \\ \parallel & & \parallel \\ \text{Spec } \mathbb{Q}_p \times Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} & \xrightarrow{\text{ev}_{I_{BC}}} & \text{Spec } \mathbb{Q}_p \times U_{\geq -n}^{\text{PL}} \\ I_{BC} \times \text{Id} \downarrow & & \downarrow I_{BC} \times \text{Id} \\ U(Z^o) \times Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m} & \xrightarrow{\text{ev}_{\text{Everywhere}}} & U(Z^o) \times U_{\geq -n}^{\text{PL}} \end{array}$$

Here $Z^1(U(Z), U_{\geq -n}^{\text{PL}})^{\mathbb{G}_m}$ denotes a certain space of \mathbb{G}_m -equivariant cocycles

$$U(Z) \rightarrow U_{\geq -n}^{\text{PL}},$$

and the maps $\text{ev}_{I_{BC}}$, $\text{ev}_{\text{Everywhere}}$ are evaluation maps. Instead of attempting to compute the scheme-theoretic image $\text{Im } \text{reg}_{\mathfrak{p}}$ directly, we compute the pullback

$$(*) \quad (I_{BC} \times \text{Id})^{-1}(\text{Im } \text{ev}_{\text{Everywhere}}).$$

1.5. The group $U(Z^o)$ possesses certain special functions, known as *motivic iterated integrals*, whose pullbacks along I_{BC} are p -adic iterated integrals. The latter may be computed to arbitrary precision thanks to the algorithm of Chatzistamatiou–Dan–Cohen [DCC]. In order to compute $\text{Im } \text{ev}_{\text{Everywhere}}$ as well as its pullback $(*)$ algorithmically, we need coordinates on $U(Z^o)$. Moreover, as the algorithm proceeds, we need to impose different, in fact contradictory, conditions on our coordinate system: to compute the pullback along I_{BC} , we need our coordinate functions to be given explicitly in terms of motivic iterated integrals. To compute the image

$$\text{Im } \text{ev}_{\text{Everywhere}}$$

however, we need coordinates compatible with the product on $U(Z^o)$. In the construction that follows, we attempt to bridge this gap; we fail in many ways, but are nevertheless able to ensure that the resulting error is computable and small.

1.6. After making precise the conjectures and theorems indicated above in §2, we begin in segments 3.1–3.2 by studying formal properties of coordinate systems on $U(Z^o)$ which promise to shrink the apparent gap between computable properties of motivic iterated integrals and the desired compatibility with product. The result, which is summarized in propositions 3.2.2 and 3.2.3, consists of conditions on a basis \mathcal{A} for the Hopf algebra $A(Z^o)$ of functions on $U(Z^o)$, given as a disjoint union of three subsets

$$\mathcal{A} = \mathcal{E} \cup \mathcal{P} \cup \mathcal{D},$$

under which

$$\mathcal{E} \cup \mathcal{P}$$

forms an algebra basis of the polynomial algebra $A(Z^o)$, and the set \mathcal{E}^\vee of dual elements forms a set of free generators for the Lie algebra

$$\mathfrak{n}(Z^o) := \text{Lie } U(Z^o).$$

Our terminology gives a rough idea of the roles played by these subsets: \mathcal{E} consists of *extensions*, \mathcal{P} of *primitive non-extensions*, and \mathcal{D} of *decomposables*.

1.7. Let $A(Z_p)$ denote the Hopf algebra of functions on $U(\mathcal{O}_p)$. Unlike the motivic Galois group $U(Z_p)$, the filtered ϕ Galois group $U(Z_p)$ possesses a canonical set of free generators which give rise, dually, to a set of *standard* basis elements in $A(Z_p)$. There is a *realization map*

$$\text{Re}_p : A(Z^o) \rightarrow \prod_{p|p} A(\mathcal{O}_p).$$

Given a motivic iterated integral in $A(Z^o)$, we may wish to expand its realization in the standard basis. In segment 3.7 we upgrade the algorithm of Chatzistamatiou–Dan-Cohen [DCC] to an algorithm which computes p -adic approximations of this expansion; we refer to this algorithm as the *realization algorithm*.

1.8. In segment 3.8 we attempt to construct a basis \mathcal{A} of iterated integrals for $A(Z^o)$ (varying $Z^o \subset Z$ as we search) which fulfills the conditions of proposition 3.2.2. One problem is that we are unable to verify algorithmically if a given iterated integral in $A(Z^o)_r$ belongs to the subspace

$$E(Z^o)_r := \text{Ext}_{\mathbf{MT}(Z)}^1(\mathbb{Q}(0), \mathbb{Q}(r)) \subset A(Z^o)_r$$

of extensions. Using the realization algorithm, however, we can bound the distance between a given iterated integral and the extension space, and so bound the error thus incurred. We are thus forced to work with two potentially distinct bases. One basis, denoted by $\tilde{\mathcal{A}}$, is given concretely and explicitly by motivic iterated integrals, but is imperfect in that its set

$$\tilde{\mathcal{E}} \subset \tilde{\mathcal{A}}$$

of alleged extensions may actually fail to be extensions. By projecting $\tilde{\mathcal{E}}$ into the space of extensions we obtain a second basis, \mathcal{A} , which is perfect in its fulfillment of the conditions of proposition 3.2.2 on the one hand, but is merely *abstract* and philosophical, on the other hand.

1.9. Let us briefly visit segment 3.8.11, where the construction becomes somewhat intricate. The construction is recursive in $n \geq 2$. As soon as we have a basis $\tilde{\mathcal{A}}_{\leq n}$ of motivic iterated integrals in half-weights $\leq n$, we want to also be able to expand an arbitrary iterated integral in half-weight n in the given basis, or, more generally, to compute the inner product of two arbitrary iterated integrals in half-weight n relative to this basis. We don't hope to be able to do this precisely; instead we aim for an ϵ -approximation

$$\langle J, I \rangle_\epsilon.$$

Segment 3.8.8 of our algorithm is key in setting the stage for this computation. Under our 'Hasse principle', the realization map is injective near the extension groups (c.f. segment 3.8.14). We may therefor require that the realization of our subset

$$\tilde{\mathcal{E}}_n \subset \tilde{\mathcal{A}}_n$$

of near-extensions be linearly independent inside $\prod A(Z_p)$; the precise statement is complicated by the fact that our realization map is itself merely an approximation. Computation of the inner products $\langle J, I \rangle_\epsilon$ for $J \in \mathcal{P}_n \cup \tilde{\mathcal{D}}_n$ reduces to computations in lower weights via the *Goncharov coproduct*, an explicit formula for the coproduct of two motivic iterated integrals first obtained by Goncharov. For the remaining inner products, $\langle J, I \rangle_\epsilon$ with $J \in \tilde{\mathcal{E}}_n$, we use the realization algorithm to map the remaining part I' of I and J into $\prod A(Z_p)$ and compute there. Our requirement that $\text{Re}_p \tilde{\mathcal{E}}_n$ be linearly independent ensures that the resulting system of linear equations will have a unique solution.

1.10. Given our abstract basis

$$\mathcal{A} = \mathcal{E} \cup \mathcal{P} \cup \mathcal{D}$$

of $A(Z^\circ)$, we obtain a set

$$\Sigma^\circ := \mathcal{E}^\vee$$

of free generators for the Lie algebra $\mathfrak{n}(Z^\circ)$. The set Φ of words in Σ° forms a basis for the universal enveloping algebra $\mathcal{U}(Z^\circ)$; its dual

$$\mathcal{F} \subset A(Z^\circ)$$

gives us a new basis, which plays nicely with the Hopf-algebra structure; we call such a basis a *shuffle basis*. We also have an exponential map

$$\exp^\sharp : U(Z^\circ) \xrightarrow{\sim} S^\bullet \mathfrak{n}(Z^\circ)^\vee$$

and we may compute the images

$$\exp^\sharp(f_w)$$

of the elements f_w of \mathcal{F} as Lie-words in Σ° . We do not endeavor to carry this out explicitly here, contenting ourselves with the observation that the procedure is in an elementary sense algorithmic.

More interesting is the need to compare the two bases \mathcal{A} and \mathcal{F} of $A(Z^\circ)$. In segment 3.9, we approximate such a comparison by using our imperfect, concrete basis $\tilde{\mathcal{A}}$ to construct a near-shuffle basis $\tilde{\mathcal{F}}$, and by computing the associated change-of-basis matrix to given p -adic precision.

1.11. In terms of a set of generators Σ^o for the unipotent motivic Galois group $U(Z^o)$, the problem of computing the image of $\mathfrak{ev}_{\text{Everywhere}}$ becomes purely formal; we make this precise in segment 4.1 below. We let \mathfrak{n}^{PL} denote the Lie algebra of the polylogarithmic quotient U^{PL} of the unipotent fundamental group of X , and we let $\mathfrak{n}(\Sigma^o)$ denote the free pronilpotent Lie algebra on Σ^o . The result is given as a finite family

$$\{F_i^{\text{abs}}\}_i$$

of elements of

$$S^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^o)_{\geq -n})^\vee.$$

1.12. We denote the natural coordinates on U^{PL} by $\log, \text{Li}_1, \text{Li}_2$, etc. In segment 4.2 we use the change-of-basis matrix of segment 3.9 to convert the elements F_i^{abs} into functions on

$$U(Z^o) \times U_{\geq -n}^{\text{PL}}$$

given as elements \tilde{F}_i of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{E}} \cup \mathcal{P}, \log, \text{Li}_1, \dots, \text{Li}_n].$$

There is a natural map

$$\mathbb{Q}[\tilde{\mathcal{E}} \cup \mathcal{P}, \log, \text{Li}_1, \dots, \text{Li}_n] \rightarrow \text{Col}(X(Z_{\mathfrak{p}}))$$

to the ring of Coleman functions, which we use to obtain the hoped-for family

$$\{\tilde{F}_i^{\mathfrak{p}}\}_i$$

of Coleman functions. Having completed the construction of the “Chabauty-Kim-loci” algorithm, $\mathcal{A}_{\text{LocI}}$, we prove our main theorem in segment 4.2.6.

1.13. In section 5 we use Newton polygons to bound the number of roots in small neighborhoods. We’re now ready to construct the point-counting algorithm of theorem 1.2.1. We search for points, to obtain a gradually increasing list

$$X(Z)_n \subset X(Z).$$

At the same time we construct Coleman functions $\tilde{F}_i^{\mathfrak{p}}$ vanishing on $X(Z_{\mathfrak{p}})_n$ and use those to obtain a gradually decreasing union of neighborhoods. Thus, roughly speaking, $X(Z)$ is sandwiched

$$X(Z)_n \subset X(Z) \subset X(Z_{\mathfrak{p}})_n$$

with $X(Z)_n$ gradually increasing while $X(Z_{\mathfrak{p}})_n$ gradually decreases. We stop when the two sides meet. This concludes the construction of our point-counting algorithm \mathcal{A}_{PC} , and allows us to state and prove the Point-Counting Theorem (segment 6.2).

1.14. In section 7 we generalize theorem 1.3.1 to allow arbitrary integer schemes. Essentially the only difference is that one is forced to replace $X(Z_{\mathfrak{p}})$ with the a product $\prod_{\mathfrak{p}|p} X(Z_{\mathfrak{p}})$. We are unable at this point, however, to obtain a point-counting algorithm in this generality: to do so we would have to study solutions to systems of locally analytic functions on higher-dimensional spaces.

1.15. **Near-term goals of explicit motivic Chabauty-Kim theory.**

1.15.1. *Algorithmic precision.* The algorithmic constructions we make in this installment are precise by mathematical standards, but not by algorithmic standards, which are far more stringent. For instance, we do not attempt to make our ϵ 's precise: any function of ϵ which is algorithmically computable, and which goes to zero with ϵ , is again denoted by ϵ — we refer to this as an *admissible change in ϵ* . Such imprecision is common in pure math, but useless for applications. Before going to Sage, we will of course have to compute exact levels of accumulated error as we make our approximations.

We also make no attempt to make our algorithm efficient: whenever we have a countable set, we don't hesitate to search through it arbitrarily. In fact, the problem of making our algorithm efficient interacts with significant, interesting problems of pure math; these include formulating explicit forms of Zagier's conjecture (available so far in only very special cases), and more precise versions of Goncharov's conjecture, at least with respect to ramification. Avoiding redundancy in our search through the set of iterated integrals is another interesting problem. Indeed, as Francis Brown has pointed out, as long as we limit ourselves to working with the polylogarithmic quotient, constructing a basis for all of $A(Z)_{\leq n}$ is huge overkill: any \mathbb{G}_m -equivariant map

$$U(Z) \rightarrow U(X)_{\geq -n}^{\text{PL}}$$

must factor through a small quotient of $U(Z)$ (easily computed in terms of abstract coordinates). A careful study of this quotient should yield a conjecture which is both much weaker than Goncharov's conjecture, and much more efficient for us.

With regard to the endeavor to produce actual code, we would expect to push the computational boundary gradually, starting with very special cases in which the conjectures of Zagier and Goncharov are relatively well understood.

1.15.2. *Comparison with Brown's method.* In the spring of 2014 I visited Francis Brown at the IHES. Shortly after my visit, he sent me a long letter in which he describes a method for constructing *many* polylogarithmic functions on the p -adic points of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ over an open subscheme of $\text{Spec } \mathbb{Z}$ which vanish on integral points, at least when there are *enough* integral points. His idea is that if Goncharov's conjecture is false, there should actually be *more* such functions available, increasing the chances of isolating the set of integral points, and his method circumvents our use of Goncharov's conjecture. I have yet to understand the exact relationship between the functions his method produces and those produced by Kim's construction. I hope the content of his letter will find its way into an article in the near future.

1.15.3. *Beyond totally real fields.* Most of the work completed here applies to arbitrary integer schemes which obey *Kim vs. Hasse*. For the final application, however, we are limited to the totally real case. As mentioned above, in order to go further, we would have to develop methods for computing solutions to systems of polylogarithmic functions in higher dimensions.

1.15.4. *Beyond the polylogarithmic quotient.* Beyond the polylogarithmic quotient, the motivic Selmer variety

$$H^1(G(Z), U(X)_{\geq -n})$$

is still canonically isomorphic to the space

$$Z^1(U(Z), U(X)_{\geq -n})^{\mathbb{G}_m}$$

of \mathbb{G}_m -equivariant cocycles. Explicit computation of this space is complicated however by the fact that the action of $U(Z)$ on $U(X)$ is highly nontrivial. This task is urgent for at least two reasons. Obviously, replacing the polylogarithmic quotient with the full unipotent fundamental group in our current algorithm would enable us to weaken our version of Kim's conjecture. More interesting, perhaps, would be the possibility of going beyond our three punctures $\{0, 1, \infty\}$ to more general punctures, including possibly punctures that are not rational over the base-field in the context of mixed Artin-Tate motives.

1.16. Acknowledgements. I would like to thank Stefan Wewers for helpful conversations during the conference on multiple zeta values in Madrid in December of 2014. I would like to thank Minhyong Kim, Amnon Besser, Francis Brown, Francesc Fit  , and Go Yamashita for helpful conversations and email exchanges. I would like to thank Cl  ment Dupont for long conversations during our time in Sarri  s, and for pointing out a very helpful counterexample (see the appendix). I would like to thank Rodolfo Venerucci for conversations about finite cohomology. I would like to thank Jochen Heinloth and Giuseppe Ancona for help improving my presentation of the results. I would like to thank David Corwin for a careful reading and many helpful comments.

2. CONJECTURES AND THEOREMS

We begin with a brief review of background material (unipotent fundamental group, Kim's conjecture, motivic iterated integrals, filtered ϕ iterated integrals, p -adic periods). For a more detailed exposition, tailored specifically to our applications, we refer the reader to Dan-Cohen–Wewers [DCW2].

2.1. A motivic variant of Kim's construction.

2.1.1. The prounipotent completion of the fundamental group has a motivic precursor, known as the *unipotent fundamental group*. We use the tangent vector 1_0 as base-point, and denote the resulting group simply by $U(X)$. The unipotent fundamental group of \mathbb{G}_m is equal to (the covariant total space of) $\mathbb{Q}(1)$. The natural inclusion

$$\mathbb{P}^1 \setminus \{0, 1, \infty\} \hookrightarrow \mathbb{G}_m$$

induces a surjection of unipotent fundamental groups

$$U(X) \twoheadrightarrow \mathbb{Q}(1).$$

Let N denote its kernel. Then according to Deligne [Del1], the Lie algebra of

$$U(X)^{\text{PL}} := U(X)/[N, N]$$

is canonically a semidirect product

$$\mathfrak{n}(X)^{\text{PL}} = \mathbb{Q}(1) \ltimes \prod_{i=1}^{\infty} \mathbb{Q}(i).$$

We write $\mathfrak{n}(X)_{\geq -n}^{\text{PL}}$ for the quotient

$$\mathbb{Q}(1) \ltimes \prod_{i=1}^n \mathbb{Q}(i),$$

of $\mathfrak{n}(X)^{\text{PL}}$, and $U_{\geq -n}^{\text{PL}}$ for the corresponding quotient of $U(X)$.

2.1.2. Sending a point $b \in X(Z)$ to the torsor of *polylogarithmic paths* $({}_bP_{10})_{\geq -n}^{\text{PL}}$ defines a map

$$\kappa : X(Z) \rightarrow H^1(U_{\geq -n}^{\text{PL}})$$

to a finite-type affine \mathbb{Q} -scheme which parametrizes such torsors, the *polylogarithmic Selmer variety*. There is also a local p -adic version. We fix a prime \mathfrak{p} of Z which we assume to be totally split for simplicity. We obtain a map

$$\kappa_{\mathfrak{p}} : X(\mathcal{O}_{\mathfrak{p}}) \rightarrow H^1(U_n^{\text{PL}, F\phi})$$

to the *filtered- ϕ polylogarithmic Selmer variety*. Connecting the filtered- ϕ and motivic versions is a map we call *unipotent syntomic regulator*, which forms a commuting square

$$\begin{array}{ccc} X(Z) & \longrightarrow & X(\mathcal{O}_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ \mathbb{Q}_p \otimes H^1(U_{\geq -n}^{\text{PL}}) & \xrightarrow{\text{reg}_{\mathfrak{p}}} & H^1(U_{\geq -n}^{\text{PL}, F\phi}). \end{array}$$

2.1.3. We define the *polylogarithmic Chabauty-Kim locus at level n* by

$$X(\mathcal{O}_{\mathfrak{p}})_n := \kappa_{\mathfrak{p}}^{-1}(\text{Im reg}_{\mathfrak{p}}),$$

to be regarded as a (not necessarily reduced) *Coleman-analytic space*. The polylogarithmic Chabauty-Kim loci form a nested sequence

$$X(\mathcal{O}_{\mathfrak{p}}) \supset X(\mathcal{O}_{\mathfrak{p}})_1 \supset X(\mathcal{O}_{\mathfrak{p}})_2 \supset \cdots \supset X(Z).$$

We note the following theorem, which is a direct consequence of the results of Kim [Kim2] via Soulé's étale regulator isomorphism [Sou].

Theorem (Kim). Suppose Z is a totally real integer scheme and let $\mathfrak{p} \in Z$ be any prime. Then for n sufficiently large, $\text{Im reg}_{\mathfrak{p}}$ is contained in a subscheme of $H^1(U_{\geq -n}^{\text{PL}, F\phi})$ of strictly lower dimension.

Recall from Kim [Kim1] that the map $\kappa_{\mathfrak{p}}$ has dense image, and pulls back algebraic functions to Coleman functions. So as soon as we have a nonzero function on $H^1(U_{\geq -n}^{\text{PL}, F\phi})$ vanishing on $\text{Im reg}_{\mathfrak{p}}$, the associated locus will be finite:

Corollary (Kim). Suppose Z is a totally real integer scheme, and assume $\mathfrak{p} \in Z$ is totally split. Then for n sufficiently large, the associated polylogarithmic Chabauty-Kim locus $X(\mathcal{O}_{\mathfrak{p}})$ is finite.

Stretching Kim's conjecture from [BDCKW] somewhat, we propose the following.

Conjecture 2.1.4 (Convergence of polylogarithmic loci). Let Z be a totally real integer scheme, and $\mathfrak{p} \in Z$ a totally split prime. Then for n sufficiently large, the associated polylogarithmic Chabauty-Kim locus satisfies

$$X(\mathcal{O}_{\mathfrak{p}})_n = X(Z).$$

The generalization from the rational to the totally real case should be harmless. By restricting attention to the polylogarithmic quotient, however, we are relying on a proper strengthening of Kim's conjecture. Nevertheless, since the codimension of $\text{Im reg}_{\mathfrak{p}}$ goes to infinity already for the polylogarithmic quotient, much of the motivation for Kim's conjecture does hold for the polylogarithmic quotient; indeed, this contention has been validated, at least unofficially, by the author of the original conjecture himself.

2.2. Iterated integrals, p -adic periods, statement of arithmetic conjectures.

2.2.1. We begin with those properties of mixed Tate motives that we use. Let Z be an integer scheme, and let $\mathbf{MT}(Z)$ denote the category of (unramified) mixed Tate motives over Z with \mathbb{Q} -coefficients.

$\mathbf{MT}(Z)$ is \mathbb{Q} -Tannakian. It has a special object $\mathbb{Q}(1)$ of rank 1. Every simple object is isomorphic to a unique $\mathbb{Q}(n) := \mathbb{Q}(1)^{\otimes n}$. Each object is equipped with an increasing filtration W , the *Weight filtration*. (Since all the weights that occur are even, we also work with *half-weights*, which are half the usual weights. These will be denoted by subscripts.) The functor

$$\mathbf{MT}(Z) \rightarrow \mathbf{Vect}(\mathbb{Q})$$

sending

$$E \mapsto \bigoplus \mathrm{Hom}(\mathbb{Q}(i), \mathrm{gr}_{-2i}^W E)$$

is a \mathbb{Q} -valued fiber functor, with associated group of the form

$$G(Z) = U(Z) \rtimes \mathbb{G}_m$$

with $U(Z)$ free pronipotent. From generalities of mixed Tate categories, we have canonical isomorphisms

$$U(Z)^{\mathrm{ab}} = \bigoplus_i \mathrm{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))^{\vee}.$$

We have (highly nontrivial) canonical isomorphisms

$$K_{2n-1}^{(n)}(Z) \xrightarrow{\sim} \mathrm{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n)),$$

and a computation of the dimensions of these K -groups via real-analytic methods due to Borel [Bor1, Bor2]:

$$\dim K_{2n-1}^{(n)}(Z) = \begin{cases} r_1 + r_2 & \text{for } n \text{ odd } \geq 3 \\ r_2 & \text{for } n \text{ even } \geq 2, \end{cases}$$

where r_1 (resp. r_2) denotes the number of real (resp. complex) places.

We let $\mathfrak{n}(Z)$ denote the Lie algebra of $U(Z)$, $\mathcal{U}(Z)$ its completed universal enveloping algebra, and $A(Z)$ the coordinate ring of $U(Z)$.

2.2.2. Our discussion of iterated integrals applies to the complement in \mathbb{P}^1 of any divisor \mathbf{D} which is étale over Z ; we continue to use the letter X . We assume $\infty \in \mathbf{D}$. The category of mixed motivic sheaves over X , equipped with a base-point a , gives rise similarly to a group $G_a(X)$. By work of Levine [Lev], the unipotent fundamental group fits into a split exact sequence

$$1 \rightarrow U_a(X) \rightarrow G_a(X) \rightarrow G(Z) \rightarrow 1.$$

2.2.3. After forgetting the $G(Z)$ -action, $U(X)$ doubles as the fundamental group of the category of unipotent vector bundles with integrable connection. A study of this category (carried out by Deligne [Del1]) shows that each unipotent path torsor is trivialized by a special path

$${}_b p_a^{\mathrm{dR}} \in {}_b P_a(\mathbb{Q})$$

and that the fundamental group is free on the set of logarithmic vector fields dual to the 1-forms

$$\omega_c = \frac{dt}{t - c}$$

for $c \in \mathbf{D}_f := \mathbf{D} \setminus \infty$. If $\omega = (\omega_1, \dots, \omega_r)$ is a sequence of such differential forms, we let f_ω denote the associated function (see section 2 of [DCW2] for generalities on free pronipotent groups).

We say that the datum $(a; \omega; b)$ is *combinatorially unramified* if the associated reduced divisors are étale over Z .¹ We let \mathbf{D} denote the reduced divisor on \mathbb{A}^1 associated to a, ω, b , excluding tangential base-points. Being combinatorially unramified has the effect that the entire path bimodule $\mathcal{U}_b P_a$ (= bimodule over completed universal enveloping algebras at a and b) is unramified over Z .

2.2.4. Following Goncharov [Gon3], we define $I_a^b(\omega)$ to be the composite

$$U(Z) \xrightarrow{o(bP_a^{\text{dR}})} {}_b P_a(X) \xrightarrow{\sim} U_a(X) \xrightarrow{f_\omega} \mathbb{A}_{\mathbb{Q}}^1.$$

If $A(Z)$ denotes the graded hopf algebra $\mathcal{O}(U(Z))$ then $I_a^b(\omega)$ belongs to $A(Z)_r$. We refer to these elements as (*combinatorially unramified*) *unipotent iterated integrals*. Among the unipotent iterated integrals are the *classical unipotent polylogarithms*:

$$\text{Li}_{n+1}^U(t) := I_{1_0}^t(0^n, 1)$$

(where the comma is used as a typographical pun to denote the concatenation product) and their single valued cousins $\text{Li}_n^{U,sv}(t)$, for which we refer the reader to Brown [Bro1]. In terms of these objects, we may state the conjectures of Zagier and Goncharov as follows.

Conjecture 2.2.5 (Zagier's conjecture). For each $n \geq 2$, the motivic Ext group

$$E_n := \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(n))$$

is spanned by single valued unipotent n -logarithms $\text{Li}_n^{U,sv}(t)$ with $t \in K$.

We recall that Zagier's conjecture is known for $n = 2$ by Zagier [Zag] and independently by work of Suslin [Sus] and Bloch [Blo], for $n = 3$ by Goncharov, and for K cyclotomic by Beilinson [Bei]. The main algorithm we construct below could be greatly simplified in the cyclotomic case $K = \mathbb{Q}(\zeta_N)$, where a basis for E_n is given explicitly by the elements $\text{Li}_n^{U,sv}(\zeta_N^i)$ for $0 < i < N/2$. Conversely, away from the cyclotomic case, our algorithm is made complicated partly because of the lack of explicit constructions, even conjectural, of elements of E_n . Away from the roots of unity, most $\text{Li}_n^{U,sv}(t)$'s are *not* contained in E_n .

Conjecture 2.2.6 (Goncharov-exhaustion). For any integer scheme Z and any $n \in \mathbb{N}$, there is an open subscheme $Z^o \subset Z$ such that $A(Z^o)_{\leq n}$ is spanned by combinatorially unramified unipotent iterated integrals over Z^o .

This conjecture represents the statement made by Goncharov [Gon2], strengthened somewhat to include weak control over ramification. Better control over ramification would yield a faster algorithm. The case $Z = \text{Spec } \mathbb{Z} \setminus \{2\}$, $n = \infty$ established by Deligne [Del2], and the discussion of the case $n = 2$ in [DCW2] both support the belief that unipotent iterated

¹By a *base-point*, we mean either an integral point, or a nowhere vanishing tangent vector at a missing point. If a is a base-point, we let a_0 denote the *location* of a : $a_0 = a$ if a is an integral point, otherwise a is a tangent vector at a_0 . We assume that the datum $(a; \omega; b)$ behaves nicely over Z in an obvious sense, which requires several cases to state precisely: in all cases we assume the reduced divisor associated to ω, a_0, b_0 , and ∞ is étale over Z ; if a is a tangent vector and $a_0 \neq b_0$, we assume the reduced divisor which supports $a + 0 + \infty$ on \mathbb{P}^1 is étale over Z ; if a, b are both tangent vectors at the same point $a_0 = b_0$, we assume similarly that the support of $a + b + 0 + \infty$ is étale over Z .

integrals should be compatible with ramification, at least to the extent predicted by our wording of the conjecture.

2.2.7. Unipotent iterated integrals have a filtered ϕ variant at each prime $\mathfrak{p} \in Z$. We mention only a few key similarities and differences, referring the reader to [DCW2] for details. As for mixed Tate motives, there is a Tannakian (in fact, mixed Tate) category of mixed Tate filtered ϕ modules, and an associated proalgebraic group of the form

$$G(\mathcal{O}_{\mathfrak{p}}) = \mathbb{G}_m \ltimes U(\mathcal{O}_{\mathfrak{p}})$$

with $U(\mathcal{O}_{\mathfrak{p}})$ free pronipotent, but now over \mathbb{Q}_p ; we adopt our notation $(\mathfrak{n}(\mathcal{O}_{\mathfrak{p}}), \mathcal{U}(\mathcal{O}_{\mathfrak{p}}), A(\mathcal{O}_{\mathfrak{p}}))$ from the motivic case.² Unlike the motivic case, $U(\mathcal{O}_{\mathfrak{p}})$ possesses canonical generators $v_{\mathfrak{p},-1}, v_{\mathfrak{p},-2}, v_{\mathfrak{p},-3}, \dots$, and an associated special $K_{\mathfrak{p}}$ -valued point

$$u_{\mathfrak{p}} = \exp \sum_i v_{\mathfrak{p},i}$$

of $U(\mathcal{O}_{\mathfrak{p}})$.

2.2.8. There is a morphism of unipotent groups (linear over $\mathrm{Spec} \mathbb{Q} \leftarrow \mathrm{Spec} \mathbb{Q}_p$)

$$U(Z) \leftarrow U(Z_{\mathfrak{p}})$$

induced by filtered ϕ realization. The composite

$$U(Z) \leftarrow U(Z_{\mathfrak{p}}) \xleftarrow{u_{\mathfrak{p}}} \mathrm{Spec} K_{\mathfrak{p}}$$

is the map denoted I_{BC} above; we refer to it as “Besser-Coleman integration”. The associated map of rings

$$\mathrm{per}_{\mathfrak{p}} := I_{\mathrm{BC}}^{\sharp} : A(\mathcal{O}_{\mathfrak{p}}) \rightarrow K_{\mathfrak{p}}$$

is called the *p-adic period map*. If π denotes the embedding of K in $K_{\mathfrak{p}}$, then we have

$$I_a^b(\omega)(I_{\mathrm{BC}}) = \mathrm{per}_{\mathfrak{p}}(I_a^b(\omega)) = \int_{a^{\pi}}^{b^{\pi}} \omega^{\pi},$$

a *p*-adic iterated integral in the sense of Coleman-Besser. (From this point of view, it’s better to think of $I_a^b(\omega)$ as a “motivic iterated *integrand*”: when we combine a *motivic iterated integrand* with *p-adic integration*, we obtain a *p-adic iterated integral*.) An algorithm for computing such integrals to arbitrary *p*-adic precision is constructed in Dan-Cohen–Chatzistamatiou [DCC]. The following conjecture is stated for instance in Yamashita [Yam].

Conjecture 2.2.9 (*p*-Adic period conjecture). Let Z be an integer scheme with fraction field K , and let \mathfrak{p} be a closed point of Z . Then the *p*-adic period map

$$\mathrm{per}_{\mathfrak{p}} : A(Z) \rightarrow K_{\mathfrak{p}}$$

is injective.

²Our use of $\mathcal{O}_{\mathfrak{p}}$ (in place of $K_{\mathfrak{p}}$) in the notation expresses the fact that we’re working with filtered ϕ -modules as opposed to filtered ϕ, N -modules.

2.2.10. *Hasse principle for finite cohomology.* In addition to the semilinear injectivity of the period conjecture, we will also need a linear injectivity property which concerns the product of syntomic regulators

$$\mathrm{reg}_p : \mathbb{Q}_p \otimes \mathrm{Ext}_{\mathcal{O}_K}^1(\mathbb{Q}(1), \mathbb{Q}(n)) \rightarrow \prod_{\mathfrak{p}|p} \mathrm{Ext}_{\mathcal{O}_{\mathfrak{p}}}^1(\mathbb{Q}_p(1), \mathbb{Q}_p(n)).$$

We recast this in the language of finite Galois cohomology as follows. Following Bloch–Kato [BK], we write $H_{\mathcal{O}_{K,f}}^i$ for cohomology classes which are unramified away from p and crystalline at all primes above p . We consider the following condition on a number field K and a prime p of \mathbb{Z} :

Condition 2.2.11. The map

$$\mathrm{loc}_p : H_{\mathcal{O}_{K,f}}^1(\mathrm{Spec} K, \mathbb{Q}_p(n)) \rightarrow \prod_{\mathfrak{p}|p} H_f^1(\mathrm{Spec} K_{\mathfrak{p}}, \mathbb{Q}_p(n))$$

is injective.

Let Z be a totally real integer scheme with function field K and assume the corresponding polylogarithmic Chabauty–Kim loci converge at n . We say that Z *obeys Kim vs. Hasse* if the above injectivity holds at levels $n' \leq n$.

To give an idea of how restrictive this condition might be, we record the following proposition, which was pointed out to me by Minhyong Kim.

Proposition. In the situation and the notation of segments 2.2.10–2.2.11, the map loc_p is injective for all but finitely many n .

We also note that this injectivity is related to the non-vanishing of certain p -adic L -values; c.f. theorem 4.2.1 of Perrin-Riou [PR].

2.3. Outline of algorithm.

2.3.1. Our main construction is an algorithm, which we denote by $\mathcal{A}_{\mathrm{LocI}}$, which takes as input an integer scheme Z , a prime p of \mathbb{Z} over which Z is totally split, a natural number n , and an ϵ , and returns an open subscheme Z° of Z , an algebra basis $\tilde{\mathcal{B}}$ of the polynomial ring $A(Z^\circ)_{\leq n}$, and a family $\{\tilde{F}_i\}_i$ of elements of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \mathrm{Li}_1, \dots, \mathrm{Li}_n].$$

2.3.2. According to [DCW2, §5.2], we have

$$\begin{aligned} H^1(G(Z), U(X)_{\geq -n}^{\mathrm{PL}}) &= Z^1(U(Z), U(X)_{\geq -n}^{\mathrm{PL}})^{\mathbb{G}_m} \\ &= \mathrm{Hom}(U(Z), U(X)_{\geq -n}^{\mathrm{PL}})^{\mathbb{G}_m}, \end{aligned}$$

the space of \mathbb{G}_m -equivariant homomorphisms, and similarly for the filtered ϕ version. Moreover, evaluation at $u_{\mathfrak{p}}$ induces an isomorphism

$$\mathrm{ev}_{u_{\mathfrak{p}}} : \mathrm{Hom}(U(Z_{\mathfrak{p}}), U(X_{\mathfrak{p}})_{\geq -n}^{\mathrm{PL}})^{\mathbb{G}_m} \xrightarrow{\sim} U(X_{\mathfrak{p}})_{\geq -n}^{\mathrm{PL}} = \mathbb{Q}_p \otimes U(X)_{\geq -n}^{\mathrm{PL}}.$$

The composit

$$\mathbb{Q}_p \otimes \mathrm{Hom}(U(Z), U(X)_{\geq -n}^{\mathrm{PL}})^{\mathbb{G}_m} \rightarrow \mathbb{Q}_p \otimes U(X)_{\geq -n}^{\mathrm{PL}}$$

is given by evaluation at the pullback I_{BC} of $u_{\mathfrak{p}}$ to $U(Z)$. As explained in the introduction, in order to compute its scheme-theoretic image, we first put this evaluation map inside the universal family of evaluation maps

$$\mathbf{ev} = \mathbf{ev}_{\text{Everywhere}} : \text{Hom}^{\mathbb{G}_m}(U(Z), U(X)_{\geq -n}^{\text{PL}}) \times U(Z^o) \rightarrow U(X)_{\geq -n}^{\text{PL}} \times U(Z^o)$$

pulled back along

$$U(Z^o) \twoheadrightarrow U(Z).$$

If we fix arbitrary generators of $U(Z^o)$, these give rise to coordinates on $A(Z^o)$, which we refer to as *abstract shuffle-coordinates*. In terms of these, the computation is purely formal. We must then however switch to coordinates whose image under the period map can be computed, that is, to *concrete coordinates* given by unipotent iterated integrals. As explained in the introduction, the heart of our algorithm constructs such coordinates, as well as an approximate change-of-basis matrix which relates a judicious choice of abstract shuffle-coordinates to our concrete coordinates. This key step is inspired by the work of Francis Brown in [Bro2].

2.4. Statement of main theorem. For each prime \mathfrak{p} lying above p , the \mathfrak{p} -adic period map extends in an obvious way to a map

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \text{Li}_1, \dots, \text{Li}_n] \rightarrow \text{Col}(X(\mathcal{O}_{\mathfrak{p}}))$$

to the ring of Coleman functions; denote the image of the element \tilde{F}_i from segment 2.3.1 by $\tilde{F}_i^{\mathfrak{p}}$.

Theorem 2.4.1. Let Z be an integer scheme, $\mathfrak{p} \in Z$ a totally split prime, p the image of \mathfrak{p} in $\text{Spec } \mathbb{Z}$, n a natural number, and $\epsilon \in p^{\mathbb{Z}}$. Let

$$\mathcal{K}_{\mathfrak{p}}(\mathfrak{n}_{\geq -n}^{\text{PL}}) \triangleleft \text{Col}(X(Z_{\mathfrak{p}}))$$

denote the ideal which defines the Chabauty-Kim locus $X(Z_{\mathfrak{p}})_n$; we refer to $\mathcal{K}_{\mathfrak{p}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ as the *p-adic Chabauty-Kim ideal associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$* .

- (1) Suppose $\mathcal{A}_{\text{Loc}}(Z, p, n, \epsilon)$ halts. Then there are functions $\{F_i^{\mathfrak{p}}\}$ generating the \mathfrak{p} -adic Chabauty-Kim ideal $\mathcal{K}_{\mathfrak{p}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$, such that

$$\left| \tilde{F}_i^{\mathfrak{p}} - F_i^{\mathfrak{p}} \right| < \epsilon$$

for all i .

- (2) Suppose Zagier's conjecture (conjecture 2.2.5) holds for K and $n' \leq n$. Suppose Goncharov exhaustion (conjecture 2.2.6) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (condition 2.2.11) in half-weights $2 \leq n' \leq n$. Then the computation $\mathcal{A}_{\text{Loc}}(Z, p, n, \epsilon)$ halts.

We remark that part (1) of the theorem is independent of the choice of norm on the space of polylogarithmic functions up to an admissible change in ϵ .

3. CONSTRUCTION OF ARITHMETIC ALGORITHMS

3.1. Generators for graded free algebras.

Proposition 3.1.1. Let $S = \bigcup_{i=1}^{\infty} S_i$ be a disjoint union of finite sets, and similarly

$$S' = \bigcup_{i=1}^{\infty} S'_i.$$

Let k be a field and $k[S], k[S']$ associated graded free algebras and I, I' the augmentation ideals. Let

$$\phi : k[S'] \rightarrow k[S]$$

be a homomorphism which preserves the grading. Suppose the induced map

$$I'/I'^2 \rightarrow I/I^2$$

is iso. Then ϕ is iso.

Proof. For $n \geq 1$, we have $I_n = k[S]_n$. Surjectivity follows by induction using the short exact sequences

$$0 \rightarrow (I^2)_n \rightarrow k[S]_n \rightarrow (I/I^2)_n \rightarrow 0.$$

Since S_i maps to a basis of $(I/I^2)_i$, the bijection

$$(I'/I'^2)_i \rightarrow (I/I^2)_i$$

gives us a bijection between S'_i and S_i . For any n , ϕ maps $S'_{\leq n}$ into $k[S]_{\leq n}$, so ϕ restricts to a map

$$k[S'_{\leq n}] \rightarrow k[S_{\leq n}]$$

of subalgebras generated in degrees $\leq n$. These are surjective maps of polynomial algebras of same finite Krull dimension. This means that

$$\text{Spec } k[S_{\leq n}] \rightarrow \text{Spec } k[S'_{\leq n}]$$

is a closed immersion between affine spaces of same dimension, hence an isomorphism by the Hauptidealsatz. \square

3.2. Generators for mixed Tate groups.

3.2.1. For a review of free pronipotent groups, we refer the reader to §2 of Dan-Cohen–Wewers [DCW2]. By a *mixed Tate group* over a field k of characteristic zero, we mean a free pronipotent group U equipped with a grading of the Lie algebra

$$\mathfrak{n} = \text{Lie } U$$

such that $\mathfrak{n}_i = 0$ for $i \geq 0$. The grading on \mathfrak{n} induces also a grading of the completed universal enveloping algebra $\mathcal{U} = \mathcal{U}\mathfrak{n}$ such that $\mathcal{U}_0 = k$ and $\mathcal{U}_i = 0$ for $i > 0$, as well as a grading on the coordinate ring $A = \mathcal{O}(U) = \mathcal{U}^\vee$ such that $A_0 = k$ and $A_i = 0$ for $i < 0$. We refer to the graded degree of an element (of $\mathfrak{n}, \mathcal{U}, A$) as its *half-weight*.

The comultiplication cuts out a vector subspace

$$E_n \subset A_n,$$

the space of *extensions*. Indeed, by the general theory of mixed Tate categories we have exact sequences

$$0 \rightarrow \text{Ext}_{\mathbf{Rep}(\mathbb{G}_m \ltimes U)}^1(k(0), k(n)) \rightarrow A_n \rightarrow \bigoplus_{\substack{i+j=n \\ i,j \geq 1}} A_i \otimes A_j$$

where $k(i)$ denotes the trivial U -representation in half-weight $-i$. Similarly, the multiplication gives rise to a subspace

$$A_n \supset D_n,$$

namely the image of the map

$$A_n \leftarrow \bigoplus_{\substack{i+j=n \\ i,j \geq 1}} A_i \otimes A_j;$$

we refer to D_n as the *space of decomposable elements*.

Proposition 3.2.2. Let U be a mixed Tate group, and let A denote its coordinate ring. For each i let E_i denote the space of extensions in A_i , D_i the space of decomposable elements. Let \mathcal{P}_i be a linearly independent subset of A_i which spans a subspace P_i complementary to $E_i + D_i$. Let \mathcal{E}_i be a basis for E_i and let $\mathcal{E} = \bigcup \mathcal{E}_i$, $\mathcal{P} = \bigcup \mathcal{P}_i$. Then as a ring,

$$A = k[\mathcal{E} \cup \mathcal{P}].$$

Proof. The subspaces E_i and D_i are disjoint. To see this, fix an arbitrary set of free generators ϵ' for U , and for w a word in ϵ' , let $f_w \in A$ denote the associated function. Then E_i has basis

$$\{f_a \mid a \in \epsilon'_{-i}\}$$

dual to the set of one-letter words of half-weight $-i$, while D_i is spanned by shuffle products of functions f_w with w a word in $\epsilon'_{>-i}$, so is contained in the space with basis

$$\{f_w \mid w \in \text{Words}_{-i}(\epsilon'_{>-i})\}.$$

It follows that A_i decomposes as a direct sum

$$(3.2.2*) \quad A_i = E_i \oplus P_i \oplus D_i$$

and that $\mathcal{E}_i \cup \mathcal{P}_i$ maps to a basis of $(I/I^2)_i$. Hence, by Proposition 3.1.1, $\mathcal{E} \cup \mathcal{P}$ forms a set of free k -algebra generators for A . \square

Proposition 3.2.3. In the situation and the notation of Proposition 3.2.2, let

$$\epsilon_{-i} \subset \mathcal{U}_{-i}$$

be dual to \mathcal{E}_i relative to the decomposition (3.2*). Then

$$\epsilon := \bigcup_{i=1}^{\infty} \epsilon_{-i}$$

forms a set of free generators for U .

Proof. We claim that every element

$$\epsilon_{-i,j} \in \epsilon_{-i}$$

is of Lie type: if

$$\nu : \mathcal{U} \rightarrow \mathcal{U} \otimes \mathcal{U}$$

denotes the comultiplication, then

$$(*) \quad \nu(\epsilon_{-i,j}) = 1 \otimes \epsilon_{-i,j} + \epsilon_{-i,j} \otimes 1.$$

Let

$$\mathcal{P}'_i = \mathcal{E}_i \cup \mathcal{P}_i.$$

According to Proposition 3.2.2, the set \mathcal{D}_i of monomials in $\mathcal{P}'_{<i}$ forms a basis of D_i . Let

$$\mathcal{A}_i = \mathcal{E}_i \cup \mathcal{P}_i \cup \mathcal{D}_i.$$

It suffices to check the equality $(*)$ after pairing with an arbitrary basis element

$$\mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''}$$

of $A_{i'} \otimes A_{i''}$ with $i' + i'' = i$. We have

$$\begin{aligned} \langle \nu(\epsilon_{-i,j}), \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle &= \langle \epsilon_{-i,j}, \mathcal{A}_{i',j'} \amalg \mathcal{A}_{i'',j''} \rangle \\ &= \begin{cases} 1 & \text{if } \mathcal{A}_{i',j'} = 1 \text{ and } \mathcal{A}_{i'',j''} = \mathcal{E}_{i,j} \text{ is dual to } \epsilon_{-i,j} \\ 1 & \text{if } \mathcal{A}_{i',j'} = \mathcal{E}_{i,j} \text{ and } \mathcal{A}_{i'',j''} = 1 \\ 0 & \text{otherwise} \end{cases} \\ &= \langle 1 \otimes \epsilon_{-i,j}, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle + \langle \epsilon_{-i,j} \otimes 1, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle \\ &= \langle 1 \otimes \epsilon_{-i,j} + \epsilon_{-i,j} \otimes 1, \mathcal{A}_{i',j'} \otimes \mathcal{A}_{i'',j''} \rangle \end{aligned}$$

which shows that $\epsilon_{-i,j}$ is of Lie type as claimed.

It follows that ϵ_{-i} is a subset of the graded piece \mathfrak{n}_{-i} of the Lie algebra $\mathfrak{n} \subset \mathcal{U}$, which maps to a basis of $\mathfrak{n}_{-i}^{\text{ab}}$. It follows that ϵ forms a set of free generators as stated. \square

3.3. By an *integer scheme* we mean an open subscheme

$$Z \subset \text{Spec } \mathcal{O}_K,$$

K a number field. By a *number scheme* we mean $\text{Spec } K$, K a number field. Given Z an integer or number scheme, we let

$$A(Z) = \mathcal{O}(U(Z))$$

denote the graded Hopf algebra of unramified mixed Tate motives over Z .

3.4. Given an integer scheme Z with function field K and a unipotent iterated integral $I_a^b(c_1, \dots, c_r) \in A(K)_n$, we say that I is *combinatorially unramified over Z* if the associated reduced divisor

$$\mathbf{D} = \{a, b, c_1, \dots, c_r\}$$

is étale over Z . We denote the \mathbb{Q} -vector space of formal linear combinations of such tuples $(a; c_1, \dots, c_r; b)$ by $\text{FI}(Z)_r$, the space of *formal integrands in half-weight r* .

3.5. If k is a field equipped with an absolute value $|\cdot|$, we say that a subset of k^n is ϵ -linearly independent if each of the associated determinants is greater than ϵ .

3.6. Let Z be an integer scheme and $p \in \mathbb{Z}$ a prime such that Z is totally split above p . Recall that $A(\mathcal{O}_{\mathfrak{p}})$ denotes the graded Hopf algebra of mixed Tate filtered ϕ modules over $K_{\mathfrak{p}}$, and recall that $A(\mathcal{O}_{\mathfrak{p}})$ possesses a *standard basis*. We say that a subset

$$\mathcal{P} \subset A(Z)_n$$

is ϵ -linearly independent relative to reg if its image in $\prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})_n$ is ϵ -linearly independent with respect to the standard basis.

3.7. Realization algorithm.

3.7.1. Recall from paragraph 2.2.7 that $U(\mathcal{O}_{\mathfrak{p}})$ denotes the unipotent fundamental group of the category of mixed Tate filtered ϕ modules, that it contains a special \mathbb{Q}_p -point u , and that the family

$$v_i = (\log u)_i \in \mathfrak{n}(\mathbb{Q}_p)$$

for $i \in \mathbb{Z}_{\leq -1}$ forms a set of free generators. The associated basis of $A(\mathbb{Z}_p)$ is what we call the *standard basis*. We now construct an algorithm for evaluating an iterated integral $I_a^b(\omega)$, whose associated divisor \mathbf{D} is étale over \mathbb{Z}_p , on a word

$$w = v_{-i_r} \cdots v_{-i_2} v_{-i_1}$$

in the generators v_i to given precision ϵ . The result may be interpreted as an algorithm which takes a natural number r and an $\epsilon \in p^{\mathbb{Z}}$ as input, and returns a linear map

$$\widetilde{^U I_{\text{Std}}^{F\phi}} : \text{FI}(Z)_r \rightarrow \prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})_r$$

given explicitly by a matrix with rational entries. If

$$\text{Re} : A(Z)_r \rightarrow \prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})_r$$

denotes the realization map, and

$$^U I : \text{FI}(Z)_r \rightarrow A(Z)_r$$

denotes the map taking an integrand to the associated unipotent iterated integral, then the triangle

$$\begin{array}{ccc} \text{FI}(Z)_r & & \\ \downarrow ^U I & \searrow \widetilde{^U I_{\text{Std}}^{F\phi}} & \\ A(Z)_r & \xrightarrow{\text{Re}} & \prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})_r \end{array}$$

fails to commute by at most ϵ . Said differently, $\widetilde{^U I_{\text{Std}}^{F\phi}}$ is an approximation of the matrix representing the composite $^U I^{F\phi} := \text{Re} \circ (^U I)$ with respect to the ‘standard’ bases on source and target. For a detailed example, see segment 7.5.3 of [DCW1].

3.7.2. We first generalize our notation for a unipotent iterated integral to allow arbitrary matrix entries of the path bimodule $\mathcal{U}({}_b P_a(\mathbb{A}^1 \setminus \mathbf{D}))$. If γ is a point of $U(Z)$ and ω', ω'' are words of length n', n'' in the vector fields

$$\left\{ \left(\frac{dt}{t-a} \right)^{\vee} \right\}_{a \in \mathbf{D}},$$

we define

$$I_a^b(\omega', \omega'')(\gamma) := \langle \omega'', \gamma \omega' \rangle.$$

This makes $I_a^b(\omega', \omega'')$ an element of $A(Z)_{n''-n'}$. Each $I_a^b(\omega', \omega'')$ is in fact an ordinary unipotent iterated integral. Specifically, we have

$$I_a^b(\omega', \omega'') = \begin{cases} I_a^b(\omega''') & \text{if } \omega'' = \omega' \omega''' \\ 0 & \text{if } \omega'' \text{ is not left-divisible by } \omega'. \end{cases}$$

In this way we may regard I_a^b itself as a square-matrix with entries in $A(Z)$. With this notation, we have

$$\begin{aligned} I_a^b(\omega)(v_{-i}) &= \langle \omega, v_{-i}(b1_a) \rangle \\ &= \langle \omega, (\log I_a^b)_i(b1_a) \rangle(u), \end{aligned}$$

where the subscript i refers to the i th graded piece of the matrix, itself a matrix concentrated along the i th superdiagonal. (Of course, we have $I_a^b(\omega)(v_{-i}) = 0$ unless $i = n$.) So finally, our algorithm consists simply of the matrix calculation

$$I_a^b(\omega)(w) = \langle \omega, (\log I_a^b)_{i_r} \cdots (\log I_a^b)_{i_2} \cdot (\log I_a^b)_{i_1}(b1_a) \rangle(u)$$

coupled with our algorithm for computing p -adic iterated integrals from [DCC].

3.8. Basis algorithm.

3.8.1. We now construct an algorithm which takes as input an integer scheme

$$Z \subset \operatorname{Spec} \mathcal{O}_K,$$

a prime p of \mathbb{Z} , a natural number n , and an

$$\epsilon \in p^{\mathbb{Z}},$$

and returns the following data.

- (1) An open subscheme $Z^o \subset Z$. We write

$$\overline{S} = \{\mathfrak{q}_1, \dots, \mathfrak{q}_{\overline{s}}\}$$

for its complement.

- (2) Sets

$$\begin{aligned} \mathcal{E}_1^g &= \{\log^U \alpha_{1,1}, \dots, \log^U \alpha_{1,r_1+r_2-1}\}, \\ \mathcal{E}_1^r &= \{\log^U \beta_1, \dots, \log^U \beta_{\overline{s}}\} \end{aligned}$$

of unipotent logarithms of elements of $\mathcal{O}_{Z^o}^*$.

- (3) For each $n' \in [2, n]$,

- (a) a set of single-valued unipotent polylogarithms

$$\tilde{\mathcal{E}}_{n'} = \{\operatorname{Li}_{n'}^{U,sv}(a_{n',1}), \dots, \operatorname{Li}_{n'}^{U,sv}(a_{n',e_{n'}})\},$$

where e_m denotes the dimension of the motivic extension space

$$\operatorname{Ext}_{Z^o}^1(\mathbb{Q}(0), \mathbb{Q}(m)),$$

- (b) a set $\mathcal{P}_{n'}$ of unipotent iterated integrals of half-weight n' ,

- (c) an $\epsilon' \in p^{\mathbb{Z}}$,

- (d) an algorithm which takes a pair I, J of unipotent iterated integrals of half-weight n' as input and returns a rational number

$$\langle I, J \rangle_{\epsilon'} \in \mathbb{Q}.$$

We denote this algorithm by A_{Basis} . We first announce the meaning of its output in proposition 3.8.2; we then construct the algorithm in segments 3.8.3–3.8.11, and prove the proposition in segments 3.8.12–3.8.14.

Proposition 3.8.2. (1) Suppose $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts. Then we have:

- (a) \mathcal{E}_1^g forms a basis of $A(\operatorname{Spec} \mathcal{O}_K)_1$.

- (b) $\mathcal{E}_1^g \cup \mathcal{E}_1^r$ forms a basis of $A(Z^o)_1$.

- (c) Each $\tilde{\mathcal{B}}_{n'} := \tilde{\mathcal{E}}_{n'} \cup \mathcal{P}_{n'}$ ($n' = 2, 3, \dots, n$) forms a basis for a subspace $\tilde{B}_{n'}$ of $A(Z^o)_{n'}$ complementary to the space $D_{n'}$ of decomposables. Moreover, the space $P_{n'}$ spanned by $\mathcal{P}_{n'}$ is disjoint from the space $E_{n'}$ of extensions.
- (d) Relative to this basis, the projection $\mathcal{E}_{n'}$ of $\tilde{\mathcal{E}}_{n'}$ onto $E_{n'}$ forms a basis of $E_{n'}$.
- (e) We let $\mathcal{B}_{n'} = \mathcal{E}_{n'} \cup \mathcal{P}_{n'}$, we let $\mathcal{D}_{n'}$ denote the set of monomials in $\mathcal{B}_{<n'}$, we let

$$\mathcal{A}_{n'} = \mathcal{B}_{n'} \cup \mathcal{D}_{n'},$$

and we denote by $|\cdot|_{\mathcal{A}}$ the norm induced on $A(Z^o)_{n'}$ by the basis $\mathcal{A}_{n'}$. If $\text{Li}_{n'}^{E,sv}(a_{n',i})$ denotes the projection of $\text{Li}_{n'}^{U,sv}(a_{n',i})$ onto $E_{n'}$ then we have

$$\left| \text{Li}_{n'}^{U,sv}(a_{n',i}) - \text{Li}_{n'}^{E,sv}(a_{n',i}) \right|_{\mathcal{A}} < \epsilon'.$$

- (f) We have $\epsilon' \leq \epsilon$.
- (g) If I, J are unipotent iterated integrals of half-weight n' , and

$$\langle I, J \rangle_{\mathcal{A}}$$

denotes the inner product relative to the basis $\mathcal{A}_{n'}$, then

$$|\langle I, J \rangle_{\epsilon'} - \langle I, J \rangle_{\mathcal{A}}|_p < \epsilon'.$$

In other words, the algorithm produced as part (d) of the output of A_{Basis} computes this inner product up to precision ϵ' .

- (2) If Zagier's conjecture (conjecture 2.2.5), Goncharov exhaustion (conjecture 2.2.6) and the Hasse principle for finite cohomology (condition 2.2.11) hold for n , Z , and K , then the computation $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts.

3.8.3. We write d_G for the reduced Goncharov coproduct, regarded as a map

$$\text{FI}(Z)_r \rightarrow (\text{FI}(Z)_{>0})_r^{\otimes 2}.$$

3.8.4. The algorithm A_{Basis} searches arbitrarily through the countably-infinite set of data $(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon')$. For the rest of the construction, we fix such a datum, and construct an algorithm which returns a boolean argument, as well as a function $\langle \cdot, \cdot \rangle_{\epsilon'}$. If the boolean result is *False*, we start over with a new datum. If the boolean result is *True*, we output

$$(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon', \langle \cdot, \cdot \rangle_{\epsilon'}).$$

For the base case with $n' = 1$ we require our basis to be of the form given in the proposition, with

$$\{a_{1,1}, \dots, a_{1,r_1+r_2-1}\}$$

a basis for \mathcal{O}_K^* , and each b_i a generator for a power of \mathfrak{q}_i .

3.8.5. We assume for a recursive construction that conditions (a)–(f) have been verified in half-weights $< n'$, and that the algorithm computing the inner products $\langle I, J \rangle_{\epsilon'}$ has been constructed in half-weights $< n'$. The inner products give us maps

$$\widetilde{U I_{\tilde{\mathcal{A}}}} : \text{FI}(Z^o)_r \rightarrow A(Z^o)_r$$

and

$$\widetilde{U I_{\tilde{\mathcal{A}}}}^{\otimes 2} : \text{FI}(Z^o)_r^{\otimes 2} \rightarrow A(Z^o)_r^{\otimes 2}$$

in the form of explicit matrices with rational coefficients with respect to the bases $\mathcal{A}_{<n'}$ of iterated integrals already constructed in lower half-weights.

3.8.6. We check if the divisors associated to the iterated integrals in $\mathcal{B}_{n'}$ are étale over Z^o ; if not, we return *false*.

3.8.7. We check each element I of $\widetilde{\mathcal{E}}_{n'}$ for proximity to $E_{n'}$. To do so, we lift I to an integrand $w \in \text{FI}(Z^o)_{n'}$, compute $\widetilde{U I_{\widetilde{\mathcal{A}}}}(d_G(w))$, and check that the p -adic norm of the resulting vector is $< \epsilon'$. If not, we return *False*.

3.8.8. We check

$$\widetilde{U I_{\text{Std}}^{F\phi}}(\widetilde{\mathcal{E}}_{n'})$$

for ϵ' -linear independence in the sense of segments 3.5, 3.6 using the *realization algorithm* of segment 3.7. If this fails, we return *False*.

3.8.9. We check $d(\mathcal{P}_{n'} \cup \widetilde{\mathcal{D}}_{n'})$ for ϵ' -linear independence by lifting $\mathcal{P}_{n'}$, $\widetilde{\mathcal{D}}_{n'}$ to $\text{FI}(Z^o)$ and applying $\widetilde{U I_{\widetilde{\mathcal{A}}}^{\otimes 2}} \circ d_G$. If this fails, we return *False*.

3.8.10. We check that ϵ' is sufficiently small compared to the spread of the basis $\widetilde{\mathcal{A}}_{n'}$ that the projection onto the space $E_{n'}$ of extensions will preserve the linear independence of $\widetilde{\mathcal{A}}_{n'}$. If this fails, we return *False*. Otherwise we return *True*.

3.8.11. For the inner product in half-weight n' , it suffices to construct

$$\langle w, x \rangle_{\epsilon'}$$

for $x \in \text{FI}(Z^o)_{n'}$ arbitrary and $w \in \widetilde{\mathcal{A}}_{n'}$ a basis element. We first construct the inner products

$$\{ \langle w, x \rangle \mid w \in \mathcal{P}_{n'} \cup \widetilde{\mathcal{D}}_{n'} \}.$$

It may happen that $\widetilde{U I_{\widetilde{\mathcal{A}}}^{\otimes 2}}(d_G(w))$ is not in the span of

$$(*) \quad \widetilde{U I_{\widetilde{\mathcal{A}}}^{\otimes 2}}(d_G(\mathcal{P}_{n'} \cup \widetilde{\mathcal{D}}_{n'})).$$

Nevertheless, we may compute the projection of the former onto the latter with respect to the basis $(\widetilde{\mathcal{A}}^{\otimes 2})_{n'}$. By the linear independence of $(*)$ established in step 3.8.9 above, the resulting system of linear equations will have a unique solution.

To compute the remaining inner products

$$\{ \langle w, x \rangle_{\epsilon'} \mid w \in \widetilde{\mathcal{E}}_{n'} \},$$

we replace x by

$$x' = x - \sum_{w \in \mathcal{P}_{n'} \cup \widetilde{\mathcal{D}}_{n'}} \langle x, w \rangle_{\epsilon'} w.$$

We then compute the projection of $\widetilde{U I_{\text{Std}}^{F\phi}}(x')$ onto the span of $\widetilde{U I_{\text{Std}}^{F\phi}}(\widetilde{\mathcal{E}}_{n'})$ inside $\prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})$. The linear independence of the latter, established in segment 3.8.8 above, ensures that the resulting system of linear equations will have a unique solution.

This completes the construction of the algorithm.

3.8.12. We now prove proposition 3.8.2. Suppose as in part (1) of the proposition that $A_{\text{Basis}}(Z, p, n, \epsilon)$ halts. Parts (a), (b) are clear. For parts (c) and (d) we note that if ϵ -approximations are ϵ -linearly independent, then the actual vectors are linearly independent. Part (e) is clear, except for perhaps the admissibility of the change in ϵ' ; see segment 3.8.13 below. For part (f) we of course limit ourselves to searching through data satisfying $\epsilon' \leq \epsilon$ in the first place.

For part (g), we note that the square below, left, commutes.

$$\begin{array}{ccc} A(Z^o)_r & \xrightarrow{d} & (A(Z^o)^{\otimes 2})_r \\ \uparrow \nu_I & & \uparrow \nu_{I^{\otimes 2}} \\ \text{FI}(Z^o)_r & \xrightarrow{d_G} & (\text{FI}(Z^o)^{\otimes 2})_r \end{array} \quad \begin{array}{ccc} A(Z^o)_r & \xrightarrow{d} & (A(Z^o)^{\otimes 2})_r \\ \uparrow \widetilde{\nu_{I_{\mathcal{A}}}} & & \uparrow \widetilde{\nu_{I_{\mathcal{A}}}^{\otimes 2}} \\ \text{FI}(Z^o)_r & \xrightarrow{d_G} & (\text{FI}(Z^o)^{\otimes 2})_r \end{array}$$

Since the corresponding vertical arrows in the left and right squares differ by ϵ' , it follows that the square on the right fails to commute by at most ϵ' . This gives us the inequality of proposition 3.8.2(g) up to a possible change in ϵ' stemming from the failure of $\widetilde{\nu_{I_{\text{Stdd}}^{F\phi}}}$ to respect two splittings: the spitting of

$$\widetilde{E}_r \subset A(Z^o)_r$$

given by the complementary space $P_r \oplus D_r$ inside the source on the one hand, and the splitting of

$$\widetilde{\nu_{I_{\text{Stdd}}^{F\phi}}}(\widetilde{E}_r) \subset \prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})$$

induced by the standard basis inside the target on the other hand.³ This is clearly admissible; we omit the details.

3.8.13. Returning to part (e), we must show that our modifications of ϵ form an algorithmically computable function which goes to zero with ϵ . This is elementary, and fits into the general setting of a valued field $(k, |\cdot|)$ and linear map

$$\phi : k^m \rightarrow k^n$$

with kernel E . We claim that if

$$|\phi x| < \epsilon$$

then

$$|x - E| < C\epsilon$$

for some algorithmically computable constant C . We let W denote the image of ϕ and V the coimage, both with induced norms. For $x \in k^m$ we let \bar{x} denote its image in V , and we let $\bar{\phi}$ denote the isomorphism

$$V \xrightarrow{\sim} W$$

³In fact, to decrease the change in ϵ , we could replace the standard basis of $A(\mathcal{O}_{\mathfrak{p}})$ with a basis compatible with the decomposition of the latter into extensions, primitive non-extensions, and decomposables, as we do for $A(Z^o)$. The map $\widetilde{\nu_{I_{\mathcal{A}}}}$ would then be nearly compatible with the splittings, yielding a function which is quadratic in ϵ .

induced by ϕ . We fix a metric isomorphism $V = W$ arbitrarily (in practice this would be accomplished by constructing orthonormal bases of both spaces), and we let C^{-1} be the absolute value of the smallest eigenvalue. Then for $x \in k^m$ we have

$$\begin{aligned} |\phi x| &= |\bar{\phi} \bar{x}| \\ &\geq C^{-1} |\bar{x}| \\ &= C^{-1} |x - E|, \end{aligned}$$

independently of the choice of metric isomorphism, which establishes the claim.

3.8.14. We turn to part (2) of the proposition: the conditional halting. If the conjectures of Zagier and Goncharov hold for the given input, then our search-space includes an open subscheme $Z^o \subset Z$, a basis $\mathcal{E}_{\leq n}$ of $E_{\leq n}$ consisting of single valued unipotent ($\leq n$)-logarithms which are combinatorially-unramified over Z^o , and a linearly independent set $\mathcal{P}_{\leq n}$ of unipotent iterated integrals which are combinatorially-unramified over Z^o completing $\mathcal{E}_{\leq n} \cup \mathcal{D}_{\leq n}$ to a basis of $A(Z^o)_{\leq n}$. Our claim is that if the Hasse principle holds, then for ϵ' sufficiently small, the boolean subalgorithm evaluated on the associated datum

$$(Z^o, \mathcal{E}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon')$$

returns *True*. The map

$$\text{reg}_p : \mathbb{Q}_p \otimes \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(n)) \rightarrow \prod_{\mathfrak{p}|p} \text{Ext}_{\mathcal{O}_{\mathfrak{p}}}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n))$$

from the global motivic Ext group to the product of filtered ϕ Ext groups corresponds to the localization map of the Hasse principle through the p -adic regulator isomorphism of Soulé on the source ([Sou]) and through the Bloch-Kato exponential map ([BK]) on the target. So under the Hasse principle, the map

$$\text{Re}_p : A(Z^o)_n \rightarrow \prod_{\mathfrak{p}|p} A(\mathcal{O}_{\mathfrak{p}})_n$$

(for $n \geq 2$) is injective near the extension space E_n . For any set of linearly independent vectors in a (finite dimensional) normed vector space, there exists an ϵ such that any set of ϵ -approximations is ϵ -linearly independent. So the claim follows. This concludes the proof Proposition 3.8.2.

3.9. Change of basis algorithm.

3.9.1. We now construct an algorithm which changes the basis constructed by the basis algorithm to one which is compatible with the coproduct up to possible errors of size ϵ . This algorithm takes as input a datum $(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon, \langle \cdot, \cdot \rangle_{\epsilon})$ as in the output of the basis algorithm A_{Basis} , and outputs for each $n' \leq n$, a square matrix of size $a_{n'} \times a_{n'}$ over \mathbb{Q} . We denote this algorithm by A_{Change} and the resulting n' th matrix by

$$A_{\text{Change}}(Z^o, \tilde{\mathcal{E}}_{\leq n}, \mathcal{P}_{\leq n}, \epsilon, \langle \cdot, \cdot \rangle_{\epsilon}, n').$$

3.9.2. For each $n' \leq n$ we fix a set

$$\Sigma_{n'}^o = \{\sigma_{-n',1}, \dots, \sigma_{-n',e_{n'}}\}$$

of symbols, and define the half-weight of $\sigma_{-n',i}$ to be $-n'$. We may then speak about words in $\Sigma_{\geq -n}^o$ and about the half-weight of a word. Entries in our matrix will be indexed by pairs (I, w) , with

$$I \in \tilde{\mathcal{A}}_{n'} = \tilde{\mathcal{E}}_{n'} \cup \mathcal{P}_{n'} \cup \tilde{\mathcal{D}}_{n'}$$

($\tilde{\mathcal{D}}_n$ denoting the set of monomials in $\tilde{\mathcal{B}}_{<n} = \tilde{\mathcal{E}}_{<n} \cup \mathcal{P}_{<n}$ of half-weight n as usual), and w a word in Σ^o of half weight $-n'$. We construct the associated matrix entry $a_{I,w}$ by recursion on the length of w . We write $\tilde{\mathcal{E}}_{n'}$ as a vector

$$\tilde{\mathcal{E}}_{n'} = (\tilde{\mathcal{E}}_{n',1}, \dots, \tilde{\mathcal{E}}_{n',e_{n'}})$$

(so $\tilde{\mathcal{E}}_{n',i} = \text{Li}_{n'}^{U,sv}(a_{n',i})$ is a single-valued unipotent n' -logarithm). When $w = \sigma_{-n',i}$ is a one-letter word, we set

$$a_{I,w} = \begin{cases} 1 & \text{if } I = \tilde{\mathcal{E}}_{n',i} \\ 0 & \text{otherwise.} \end{cases}$$

Now suppose $n' = l + m$ with $l, m > 0$, and let w be a word of half-weight $-m$. Using the Goncharov coproduct and the inner product, we expand

$$d_{l,m}I = \sum c_{j,k} \tilde{\mathcal{A}}_{l,j} \otimes \tilde{\mathcal{A}}_{m,k}$$

in the basis

$$\tilde{\mathcal{A}}_l \otimes \tilde{\mathcal{A}}_m = \left\{ \tilde{\mathcal{A}}_{l,j} \otimes \tilde{\mathcal{A}}_{m,k} \right\}_{j,k}$$

of $\tilde{\mathcal{A}}_l \otimes \tilde{\mathcal{A}}_m$ to precision ϵ . In terms of the $c_{j,k}$, we define

$$a_{I, \sigma_{-l,i} \cdot w} = \sum_{j,k} c_{j,k} \cdot a_{\tilde{\mathcal{A}}_{l,j}, \sigma_{-l,i}} \cdot a_{\tilde{\mathcal{A}}_{m,k}, w}$$

which equals

$$\sum_k c_{i,k} a_{\tilde{\mathcal{A}}_{m,k}, w}$$

if we number the basis $\tilde{\mathcal{A}}_m$ in such a way that

$$\tilde{\mathcal{A}}_{m,j} = \tilde{\mathcal{E}}_{m,j}$$

for $j \in [1, e_m]$.

3.9.3. We now make the meaning of the output precise. Let $\mathcal{E}_{n,i}$ denote the projection of $\tilde{\mathcal{E}}_{n,i}$ onto the space E_n of extensions (so in the context of the basis algorithm, we have $\mathcal{E}_{n,i} = \text{Li}_n^{E,sv}(a_{n,i})$). For each n , we let $\mathcal{B}_n = \mathcal{E}_n \cup \mathcal{P}_n$, and we let \mathcal{D}_n denote the set of monomials in $\mathcal{B}_{<n}$. According to proposition 3.2.2,

$$\mathcal{A}_n := \mathcal{B}_n \cup \mathcal{D}_n$$

forms a basis of $A(Z^o)_n$. Let $\sigma_{-n,i} \in \mathcal{U}(Z^o)_{-n}$ denote the element dual to $\mathcal{E}_{n,i}$ relative to this basis. With this interpretation of the set Σ^o of symbols $\sigma_{-n,i}$, according to proposition 3.2.3, Σ^o becomes a set of free generators of the free pronipotent group $U(Z^o)$. For $w \in \mathcal{U}(Z^o)_{-n}$ a word in Σ^o of half-weight $-n$, let $f_w \in A(Z^o)_n$ denote the corresponding function.

Let $(b_{w,I})_{w,I}$ denote the inverse of the matrix constructed in the algorithm. For w a word of half-weight $-n$, define $\tilde{f}_w \in A(Z^\circ)_n$ by

$$\tilde{f}_w = \sum_{I \in \tilde{\mathcal{A}}_n} b_{w,I} I.$$

Proposition 3.9.4. In the situation and the notation above, we have

$$|f_w - \tilde{f}_w| < \epsilon.$$

Proof. This is equivalent (up to an admissible change in ϵ) to the estimate

$$|a_{I,w} - \langle w, I \rangle| < \epsilon.$$

Our algorithm is based on the following two properties of the numbers $\langle w, I \rangle$ for w a word in our set of abstract generators Σ , and I an element of our concrete basis $\tilde{\mathcal{A}}_n$:

(1) we have

$$\left| \langle \sigma_{n,i}, I \rangle - \begin{cases} 1 & \text{if } I = \tilde{\mathcal{E}}_{n,i} \\ 0 & \text{otherwise} \end{cases} \right| < \epsilon,$$

and

(2) we have

$$|\langle \sigma_{n,i} \cdot w, I \rangle - \langle \sigma_{n,i} \otimes w, dI \rangle| < \epsilon.$$

The proposition follows. \square

4. CONSTRUCTION OF GEOMETRIC ALGORITHMS

4.1. Cocycle-evaluation-image algorithm. Fix finite sets $\Sigma_{-1}, \Sigma_{-2}, \Sigma_{-3}, \dots, \Sigma_{-n}$ and $\Sigma_{-1}^\circ, \Sigma_{-2}^\circ, \Sigma_{-3}^\circ, \dots, \Sigma_{-n}^\circ$ with

$$\Sigma_{-1} \subset \Sigma_{-1}^\circ$$

and $\Sigma_i^\circ = \Sigma_i$ for $i \leq -2$. Set

$$\Sigma = \bigcup \Sigma_i, \quad \Sigma^\circ = \bigcup \Sigma_i^\circ.$$

Let $\mathfrak{n}(\Sigma), \mathfrak{n}(\Sigma^\circ)$ denote the free graded pronilpotent Lie algebras on generators Σ, Σ° . As usual, we refer to the grading as the *half-weight*. Let \mathfrak{n}^{PL} denote the polylogarithmic Lie algebra over \mathbb{Q} ,

$$\mathfrak{n}^{\text{PL}} = \mathbb{Q}(1) \ltimes \prod_{i=1}^{\infty} \mathbb{Q}(i)$$

with $\mathbb{Q}(i)$ in half-weight $-i$. We write $\text{Hom}_{\text{Lie}}^{\mathbb{G}_m}$ for homogeneous Lie-algebra homomorphisms of graded degree 0. Let ϕ denote the natural quotient map

$$\phi : \mathfrak{n}(\Sigma^\circ) \twoheadrightarrow \mathfrak{n}(\Sigma)$$

and let \mathfrak{ev} denote the map

$$\text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(\Sigma), \mathfrak{n}^{\text{PL}}) \times \mathfrak{n}(\Sigma^\circ)_{\geq -n} \rightarrow \mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^\circ)_{\geq -n}$$

given by

$$\mathfrak{ev}(\mathcal{C}, F) = (\mathcal{C}(\phi(F)), F).$$

Then \mathfrak{ev} is in an obvious sense a map of finite dimensional affine spaces, and it is straightforward to construct an algorithm which computes its scheme-theoretic image. (At the very least, this would be a standard application of elimination theory, but in fact, it should be

possible to obtain a closed formula.) We omit the details. We refer to this as the *cocycle-evaluation-image* algorithm. We denote it by $\mathcal{A}_{\text{Eval}}$, and its output, a finite list of elements of

$$S^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^\circ)_{\geq -n})^\vee,$$

by $\mathcal{A}_{\text{Eval}}(\Sigma, \Sigma^\circ, n)$.

4.2. Chabauty-Kim-loci algorithm.

4.2.1. We now construct the Chabauty-Kim-loci algorithm discussed in the introduction. As input it takes an integer scheme Z , a prime p of \mathbb{Z} , a natural number n , and an $\epsilon \in p^\mathbb{Z}$. As output it returns a finite family

$$\tilde{\mathcal{B}} = \tilde{\mathcal{E}} \cup \mathcal{P}$$

of unipotent iterated integrals, and a finite family $\{\tilde{F}_i\}_i$ of elements of the polynomial ring

$$\mathbb{Q}[\tilde{\mathcal{B}}, \log, \text{Li}_1, \text{Li}_2, \dots, \text{Li}_n],$$

which we denote by $\mathcal{A}_{\text{Loc}}(Z, p, n, \epsilon)$.

4.2.2. We run $A_{\text{Basis}}(Z, p, n, \epsilon)$. This gives us our set $\tilde{\mathcal{B}} = \tilde{\mathcal{B}}_{\leq n}$ of unipotent iterated integrals. We run $\mathcal{A}_{\text{Change}}$ on $A_{\text{Basis}}(Z, p, n, \epsilon)$ to obtain a matrix

$$M_{\leq n} = \bigoplus_{i=0}^n M_i.$$

4.2.3. We let Σ_{-1} denote a set of size $e_1 = \dim \mathcal{O}_Z^* \otimes \mathbb{Q}$, Σ_{-1}° a set containing Σ_{-1} of size $e_1^\circ = \dim \mathcal{O}_{Z^\circ}^* \otimes \mathbb{Q}$, and for each $i \in [2, n]$, $\Sigma_{-i} = \Sigma_{-i}^\circ$ a set of size

$$e_i = \dim \text{Ext}_K^1(\mathbb{Q}(0), \mathbb{Q}(i)).$$

We run $\mathcal{A}_{\text{Eval}}(\Sigma, \Sigma^\circ, n)$ to obtain a finite family $\{F_i^{\text{abs}}\}_i$ of elements of $S^\bullet(\mathfrak{n}_{\geq -n}^{\text{PL}} \times \mathfrak{n}(\Sigma^\circ)_{\geq -n})^\vee$.

4.2.4. We pull back along the quotient map

$$\mathfrak{n}(\Sigma^\circ) \twoheadrightarrow \mathfrak{n}(\Sigma^\circ)_{\geq -n}.$$

We pull back further along the logarithm

$$U(\Sigma^\circ) \rightarrow \mathfrak{n}(\Sigma^\circ)$$

Denoting the natural coordinates on \mathfrak{n}^{PL} by $\log, \text{Li}_1, \text{Li}_2, \text{Li}_3, \dots$, we obtain a finite family of elements of

$$S^\bullet \mathfrak{n}_{\geq -n}^{\text{PL}} \otimes A(\Sigma^\circ) = A(\Sigma^\circ)[\log, \text{Li}_1, \dots, \text{Li}_n]$$

which are contained in degrees $\leq n$.

4.2.5. The matrix $M_{\leq n}$ defines a linear bijection

$$A(\Sigma^\circ)_{\leq n} \xrightarrow{\sim} \mathbb{Q}[\tilde{\mathcal{B}}]_{\leq n}$$

which we use to obtain the hoped-for family $\{\tilde{F}_i\}_i$. This completes the construction of the algorithm.

4.2.6. *Proof of Theorem 2.4.1.* We have a sequence of maps

$$U(X)_{\geq -n, \mathbb{Q}_p}^{\text{PL}} \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o) \twoheadrightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n}$$

and an associated sequence of Cartesian squares:

$$\begin{array}{ccc} \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n}) & \xrightarrow{\bar{\text{ev}}_n} & \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \mathfrak{n}(Z^o)_{\geq -n} \\ \uparrow & & \uparrow \\ \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n} \times \mathfrak{n}(Z^o)) & \xrightarrow{\text{ev}_n} & \mathfrak{n}(X)_{\geq -n} \times \mathfrak{n}(Z^o) \\ \uparrow & & \uparrow \\ \text{Hom}_{\text{Lie}}^{\mathbb{G}_m}(\mathfrak{n}(Z), \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p) & \xrightarrow{\text{ev}_n(\nu_p)} & \mathfrak{n}(X)_{\geq -n}^{\text{PL}} \times \text{Spec } \mathbb{Q}_p \\ \uparrow & & \uparrow \\ \text{Hom}_{\text{Groups}}^{\mathbb{G}_m}(U(Z), U(X)_{\geq -n}^{\text{PL}})_{\mathbb{Q}_p} & \xrightarrow{\text{ev}_n(u_p)} & U(X)_{\geq -n, \mathbb{Q}_p}^{\text{PL}} \end{array}$$

Our contention is that formation of scheme-theoretic image along each horizontal map is compatible with pullback along each vertical map. We start at the top. For $\nu \in \mathfrak{n}(Z^o)$ mapping to $\bar{\nu} \in \mathfrak{n}(Z)$ and

$$\phi : \mathfrak{n}(Z) \rightarrow \mathfrak{n}(X)_{\geq -n}^{\text{PL}}$$

a \mathbb{G}_m -equivariant homomorphism, $\phi(\bar{\nu})$ depends only on the image of ν in $\mathfrak{n}(Z^o)_{\geq -n}$. So

$$\text{Im } \text{ev}_n = (\text{Im } \bar{\text{ev}}_n) \times \mathfrak{n}(Z^o)_{< -n}.$$

We go on to the middle square. By the period conjecture, $A(Z^o) \rightarrow \mathbb{Q}_p$ is flat. (In general, if A is integral, K a field, and $\psi : A \rightarrow K$ is injective, then ψ is flat, since it factors as a localization map followed by a field extension.) Hence formation of the scheme-image is compatible with pullback. Turning to the bottom square, the vertical maps are iso, so this is clear. This completes the proof of Theorem 2.4.1.

5. CONSTRUCTION OF ANALYTIC ALGORITHMS

5.1. Root criterion algorithm.

5.1.1. We now construct a boolean-valued algorithm which takes as input a boolean $b \in \{0, 1\}$, natural numbers N, r and h , and a polynomial with rational coefficients

$$\tilde{F} = \sum_{i=0}^N \tilde{a}_i T^i$$

which has at most b (\mathbb{Q}_p -rational) roots inside the disk of radius p^{-r} . We call this algorithm the *root criterion algorithm* and denote the output by $\mathcal{A}_{\text{RC}}(b, N, r, h, \tilde{F})$. We first announce the meaning of the output as a remark.

Remark 5.1.2. In our application below,

$$F = \sum_{i=1}^{\infty} a_i T^i$$

will be a power-series expansion of a polynomial in logarithms and polylogarithms of half-weight h over \mathbb{Q}_p , and \tilde{F} will be an approximation of F with arithmetic precision p^{-r} and

geometric precision e^{-N} . Suppose $\mathcal{A}_{\text{RC}}(b, N, r, h, \tilde{F}) = \text{True}$. Then F has at most b roots within the disk of radius p^{-r} . This amounts to an elementary use of Newton polygons, together with the growth estimate

$$v(a_k) \geq -h \log_p(k)$$

which follows from proposition 6.7 of Besser–de Jeu [BdJ].

5.1.3. *Case 1: $b=0$.*

- (1) If $\tilde{a}_0 = 0$, return *False*.
- (2) Compute real solutions to

$$v(\tilde{a}_0) - rt = -h \log_p t$$

to within 0.5. If there are none, return *True*.

- (3) Otherwise, there are two solutions $t_L < t_R$. If $t_R > N$, return *False*.
- (4) Check the condition

$$v(\tilde{a}_k) > v(\tilde{a}_0) - rk$$

for $1 \leq k \leq t_R$. If the condition holds, return *True*. Otherwise return *False*.

5.1.4. *Case 2.1: $b = 1$, $\tilde{a}_0 = 0$.*

- (1) If $\tilde{a}_1 = 0$, return *False*.
- (2) Compute solutions to

$$-r(t-1) + v(\tilde{a}_1) = -h \log_p t$$

to within 0.5. If there are none, return *True*.

- (3) Otherwise, there are two solutions $t_L < t_R$. If $t_R > N$, return *False*.
- (4) Check the condition

$$v(\tilde{a}_k) > -r(k-1) + v(\tilde{a}_1)$$

for $2 \leq k \leq t_R$. If this condition holds, return *True*. Otherwise, return *False*.

5.1.5. *Case 2.2: $b = 1$, $\tilde{a}_0 \neq 0$.* In this case, we have

$$(*) \quad v(\tilde{a}_1) = v(\tilde{a}_0) - r$$

and

$$(**) \quad v(\tilde{a}_0) - rt = -h \log_p t$$

has two solutions $t_L < t_R$.

- (1) If $t_R > N$, return *False*.
- (2) Check the condition

$$v(\tilde{a}_i) > v(\tilde{a}_0) - ri$$

for $2 \leq i \leq t_R$. If this condition holds, return *True*, otherwise return *False*.

6. THE POINT-COUNTING ALGORITHM

6.1. Construction of the algorithm.

6.1.1. We now construct the promised algorithm for totally real fields which obey *Kim vs. Hasse*. Our algorithm takes as input an integer scheme Z and outputs a finite set of elements of $X(Z)$. We denote the output by $\mathcal{A}_{\text{PC}}(Z)$.

6.1.2. We find a prime p of \mathbb{Z} in the image of Z , for which Z is totally split. We fix arbitrarily a prime \mathfrak{p} of Z lying above p .

6.1.3. Our algorithm searches through the set of triples (n, N, ϵ) , $n, N \in \mathbb{N}$, ϵ in a countable subset of $\mathbb{R}_{>0}$ with accumulation point 0. After each attempt, we increase n and N and decrease ϵ . To each such triple, our algorithm assigns a set $X(Z)_n$ of points of $X(Z)$ and a boolean. If the boolean output is *True*, then we output $X(Z)_n$. If the boolean output is *False*, then we continue the search.

To produce the set $X(Z)_n$, we spend n seconds searching for points. To produce the boolean output, we follow the steps described in segments 6.1.4–6.1.9 below.

6.1.4. Partition $X(\mathcal{O}_{\mathfrak{p}})$ into ϵ -balls, decreasing ϵ as needed to ensure that each ball contains at most one element of $X(Z)_n$.

6.1.5. Run $\mathcal{A}_{\text{Loc}}(Z, p, n, \epsilon)$ to obtain a family $\{\widetilde{F}_i\}_i$ of polylogarithmic functions. Set h_i equal to the half-weight of \widetilde{F}_i .

6.1.6. We focus our attention on an ϵ -ball B containing a rational representative $y \in B$. Expand each polylogarithmic function \widetilde{F}_i to arithmetic precision ϵ and geometric precision e^{-N} about y ; denote the result by $\widetilde{F}_i^{\mathfrak{p}}$.

6.1.7. Fixing i , write

$$\widetilde{F}_i^{\mathfrak{p}} = \sum_{j=0}^N \widetilde{a}_j T_j.$$

Check the following condition:

$$\text{For each } i \text{ and each } j \leq N, \text{ if } \widetilde{a}_j \neq 0 \text{ then } |\widetilde{a}_j| \geq \epsilon.$$

If this *fails*, return, *False*.

6.1.8. We continue to work with the single ϵ -ball B . Set b equal to the number of points (0 or 1) in $X(Z)_n \cap B$. Choose an $r \in \mathbb{N}$ such that $\epsilon \geq p^{-r}$. Run the root-criterion algorithm $\mathcal{A}_{\text{RC}}(b, N, r, h_i, \widetilde{F}_i^{\mathfrak{p}})$ for varying i .

6.1.9. Repeat the steps of segments 6.1.6–6.1.9 for each ϵ -ball B . If for each ball B there exists an i such that

$$\mathcal{A}_{\text{RC}}(b, N, r, h_i, \widetilde{F}_i^{\mathfrak{p}}) = \text{True},$$

return *True*. Otherwise return *False*. This completes the construction of the algorithm.

6.2. Point-counting theorem. We come to the main applications announced in the introduction.

Theorem 6.2.1. Let Z be an integer scheme with fraction field K .

(1) Suppose the algorithm $\mathcal{A}_{\text{PC}}(Z)$ halts. Then we have

$$\mathcal{A}_{\text{PC}}(Z) = X(Z).$$

(2) Assume K is totally real. Suppose Kim's conjecture (conjecture 2.1.4) holds for Z at level n . Suppose Zagier's conjecture (2.2.5) holds for K and $n' \leq n$. Suppose Goncharov's conjecture (2.2.6) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^\circ \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (condition 2.2.10) in half-weights $2 \leq n' \leq n$. Then $\mathcal{A}_{\text{PC}}(Z)$ halts.

(3) Assume $K = \mathbb{Q}$. Suppose Kim's conjecture holds for Z at level n . Suppose Goncharov's conjecture holds for Z and $n' \leq n$. Suppose the conjectured nonvanishing

$$\zeta^p(n') \neq 0$$

holds for $n' \in [3, n]$ odd. Then $\mathcal{A}_{\text{PC}}(Z)$ halts.

Proof. Parts (1) and (2) are a direct application of theorem 2.4.1. One point may require clarification: the role of segment 6.1.7. Let $\{F_i^{\mathfrak{p}}\}_i$ denote the generators of the Chabauty-Kim ideal close to $\{\tilde{F}_i^{\mathfrak{p}}\}_i$ whose existence is guaranteed by theorem 2.4.1. Fixing an ϵ -ball B with representative $y \in B$ and an i , write

$$F_i^{\mathfrak{p}} = \sum_{j=1}^{\infty} a_j T^j \quad \text{and} \quad \tilde{F}_i^{\mathfrak{p}} = \sum_{j=0}^{\infty} \tilde{a}_j T^j$$

for the power series expansions about y . Then after an admissible change in ϵ (depending on N), we have

$$|a_j - \tilde{a}_j| < \epsilon$$

for all $j \leq N$. By construction, we have

$$|\tilde{a}_j - \tilde{\tilde{a}}_j| < \epsilon,$$

hence

$$|a_j - \tilde{\tilde{a}}_j| < \epsilon.$$

For part (1) of the theorem, suppose that for given B , i and j , we find that $|\tilde{\tilde{a}}_j| \geq \epsilon$. Then by the nonarchimedean triangle inequality, we have

$$|\tilde{\tilde{a}}_j| = |a_j|.$$

This means that those valuations whose precise determination is needed for the root criterion algorithm \mathcal{A}_{RC} , will indeed be precise. For part (2), we need only note that for ϵ sufficiently small depending on N , we will indeed have for each ϵ -ball B , each i , and each $j \leq N$, either $\tilde{\tilde{a}}_j = 0$ or $|\tilde{\tilde{a}}_j| \geq \epsilon$.

For part (3), we note that the conjectured nonvanishing implies both the period conjecture and the Hasse principle in this case. \square

7. BEYOND TOTALLY REAL FIELDS

7.1. We first explain the inadequacy of the methods developed above for dealing with fields which are not totally real.

Proposition. Let Z be an integer scheme, n a natural number, $\mathfrak{p} \in Z$ a totally split prime, and $X(\mathcal{O}_{\mathfrak{p}})_n$ the associated polylogarithmic Chabauty-Kim locus. Suppose Z is not totally real, and assume the period conjecture holds. Then $X(\mathcal{O}_{\mathfrak{p}})_n = X(\mathcal{O}_{\mathfrak{p}})$.

Proof. In this case, each motivic Ext group $\mathrm{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))$ is nonzero, and by the period conjecture, each (abelian) syntomic regulator map

$$\mathrm{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n)) \rightarrow \mathrm{Ext}_{\mathcal{O}_{\mathfrak{p}}}^1(\mathbb{Q}_p(0), \mathbb{Q}_p(n))$$

is at least nonzero. Since the motivic Ext^2 -groups are nevertheless zero, the Selmer scheme $H^1(G(Z), U(X)_{\geq -n}^{\mathrm{PL}})$ is an $\mathrm{Ext}_Z^1(\mathbb{Q}(0), \mathbb{Q}(n))$ -torsor over $H^1(G(Z), U(X)_{\geq -(n-1)}^{\mathrm{PL}})$. The unipotent regulator map

$$\mathrm{reg}_{\mathfrak{p}} : H^1(G(Z), U(X)_{\geq -n}^{\mathrm{PL}}) \rightarrow H^1(G(\mathcal{O}_{\mathfrak{p}}), U(X)_{\geq -n}^{\mathrm{PL}})$$

is compatible with torsor structures. It follows by induction that $\mathrm{reg}_{\mathfrak{p}}$ is surjective, which completes the proof of the proposition. \square

7.2. Instead of considering the single unipotent regulator $\mathrm{reg}_{\mathfrak{p}}$ we may consider the product, which fits into a square similar to the one considered above

$$\begin{array}{ccc} X(Z) & \longrightarrow & \prod_{\mathfrak{p}|p} X(\mathcal{O}_{\mathfrak{p}}) \\ \downarrow & & \downarrow \alpha \\ H^1(G(Z), U(X)_{\geq -n}^{\mathrm{PL}}) & \xrightarrow{\mathrm{reg}_p} & \prod_{\mathfrak{p}|p} H^1(G(\mathcal{O}_{\mathfrak{p}}), U(X)_{\geq -n}^{\mathrm{PL}}). \end{array}$$

We define the *big polylogarithmic Chabauty-Kim locus* by

$$\left(\prod_{\mathfrak{p}|p} X(\mathcal{O}_{\mathfrak{p}}) \right)_n := \alpha^{-1}(\mathrm{Im} \mathrm{reg}_p).$$

We also write $\mathcal{K}_p^{\mathrm{Big}}(\mathfrak{n}_{\geq -n}^{\mathrm{PL}})$ for the corresponding ideal of Coleman functions, the *big p -adic Chabauty-Kim ideal*. We restrict ourselves as usual to the totally split case for simplicity.

Conjecture 7.2.1 (Kim's conjecture, general case). Let Z be an integer scheme and p a prime below Z , for which Z is totally split. For each $n \in \mathbb{N}$ let $\left(\prod_{\mathfrak{p}|p} X(\mathcal{O}_{\mathfrak{p}}) \right)_n$ denote the associated big polylogarithmic Chabauty-Kim locus. Then for some n we have

$$X(Z) = \left(\prod_{\mathfrak{p}|p} X(\mathcal{O}_{\mathfrak{p}}) \right)_n.$$

7.3. A straightforward modification of the algorithm $\mathcal{A}_{\text{Loc i}}$ yields an algorithm which produces approximate generators for the ideal of polylogarithmic functions defining the big polylogarithmic loci. Its output includes an algebra basis \mathcal{B} of $A(Z^o)_{\leq n}$ for Z^o an open subscheme of Z , as well as a family of elements \tilde{F}_i of the polynomial ring

$$\mathbb{Q}[\mathcal{B}, \{\log t_p\}_p, \{\text{Li}_i t_p\}_{i,p}].$$

We denote its output by $\mathcal{A}_{\text{Big-Loc i}}(Z, p, n, \epsilon)$. The result is a theorem which is analogous to the one stated above.

Theorem 7.3.1. Let Z be an integer scheme, p a prime over which Z is totally split, n a natural number, and $\epsilon \in p^{\mathbb{Z}}$.

- (1) Suppose $\mathcal{A}_{\text{Big-Loc i}}(Z, p, n, \epsilon)$ halts. Then there are functions $\{F_i^p\}$ generating the big p -adic Chabauty-Kim ideal $\mathcal{K}_p^{\text{Big}}(\mathfrak{n}_{\geq -n}^{\text{PL}})$ associated to $\mathfrak{n}_{\geq -n}^{\text{PL}}$ such that

$$|\tilde{F}_i^p - F_i^p| < \epsilon$$

for all i .

- (2) Suppose Zagier's conjecture (conjecture 2.2.5) holds for K and $n' \leq n$. Suppose Goncharov exhaustion (conjecture 2.2.6) holds for Z and $n' \leq n$. Suppose the period conjecture holds for the open subscheme $Z^o \subset Z$ constructed in segment 3.8 in half-weights $n' \leq n$. Suppose K obeys the Hasse principle for finite cohomology (condition 2.2.10) in half-weights $2 \leq n' \leq n$. Then the computation $\mathcal{A}_{\text{Loc i}}(Z, p, n, \epsilon)$ halts.

APPENDIX A. A MINOR ERRATUM

A.1. The article [Gon1] contains a minor error: if lemma 3.7 of that article were true, our algorithm could be greatly simplified. However, Clément Dupont has pointed out the following simple counterexample: $(\log^U 2)\zeta^U(3)$ is ramified at 2. To see this, note that $A(\text{Spec } \mathbb{Z})_4 = 0$, that $A(\text{Spec } \mathbb{Q})$ is an integral domain, and that both $\log^U 2$ and $\zeta^U(3)$ are nonzero. However, since both of these elements are contained in the space of extensions, in the notation of that article, we have $\Delta'_{[4]}((\log^U 2)\zeta^U(3)) = 0$.

REFERENCES

- [BDCKW] J. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves. Preprint. arXiv:1209.0640v1.
- [BdJ] Amnon Besser and Rob de Jeu. $\text{Li}^{(p)}$ -service? An algorithm for computing p -adic polylogarithms. *Math. Comp.*, 77(262):1105–1134, 2008.
- [Bei] AA Beilinson. Polylogarithm and cyclotomic elements. *preprint*, 1989.
- [BK] Spencer Bloch and Kazuya Kato. L -functions and Tamagawa numbers of motives. In *The Grothendieck Festschrift, Vol. I*, volume 86 of *Progr. Math.*, pages 333–400. Birkhäuser Boston, Boston, MA, 1990.
- [Blo] Spencer J. Bloch. Higher regulators, algebraic K -theory, and zeta functions of elliptic curves. 11:x+97, 2000.
- [Bor1] Armand Borel. Sur la cohomologie des espaces fibrés principaux et des espaces homogènes de groupes de Lie compacts. *Ann. of Math. (2)*, 57:115–207, 1953.
- [Bor2] Armand Borel. Cohomologie de SL_n et valeurs de fonctions zeta aux points entiers. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 4(4):613–636, 1977.
- [Bro1] Francis Brown. Single valued periods and multiple zeta values. Preprint. arXiv:1309.5309v1.
- [Bro2] Francis C. S. Brown. On the decomposition of motivic multiple zeta values. In *Galois-Teichmüller theory and arithmetic geometry*, volume 63 of *Adv. Stud. Pure Math.*, pages 31–58. Math. Soc. Japan, Tokyo, 2012.

- [DCC] Ishai Dan-Cohen and Andre Chatzistamatiou. Algorithmic computation of p -adic iterated integrals. In preparation.
- [DCW1] Ishai Dan-Cohen and Stefan Wewers. Explicit Chabauty-Kim theory for the thrice punctured line in depth two. *Proceedings of the London Math Society*. To appear. arXiv:1209.0276v1.
- [DCW2] Ishai Dan-Cohen and Stefan Wewers. Mixed tate motives and the unit equation. *International Math Research Notices*. To appear. arXiv:1311.7008.
- [Del1] Pierre Deligne. Le groupe fondamental de la droite projective moins trois points. In *Galois groups over \mathbf{Q} (Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 79–297. Springer, New York, 1989.
- [Del2] Pierre Deligne. Le groupe fondamental unipotent motivique de $\mathbf{G}_m - \mu_N$, pour $N = 2, 3, 4, 6$ ou 8 . *Publ. Math. Inst. Hautes Études Sci.*, (112):101–141, 2010.
- [Gon1] Alexander B. Goncharov. Multiple polylogarithms and mixed Tate motives. arXiv:math/0103059v4 [math.AG].
- [Gon2] Alexander B. Goncharov. Polylogarithms in arithmetic and geometry. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Zürich, 1994)*, pages 374–387, Basel, 1995. Birkhäuser.
- [Gon3] Alexander B. Goncharov. Galois symmetries of fundamental groupoids and noncommutative geometry. *Duke Math. J.*, 128(2):209–284, 2005.
- [Kim1] Minhyong Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. Res. Inst. Math. Sci.*, 45(1):89–133, 2009.
- [Kim2] Minhyong Kim. Tangential localization for Selmer varieties. *Duke Math. J.*, 161(2):173–199, 2012.
- [Lev] Marc Levine. Tate motives and the fundamental group. In *Cycles, motives and Shimura varieties*, Tata Inst. Fund. Res. Stud. Math., pages 265–392. Tata Inst. Fund. Res., Mumbai, 2010.
- [PR] Bernadette Perrin-Riou. La fonction L p -adique de Kubota-Leopoldt. 174:65–93, 1994.
- [Sou] Christophe Soulé. On higher p -adic regulators. In *Algebraic K-theory, Evanston 1980 (Proc. Conf., Northwestern Univ., Evanston, Ill., 1980)*, volume 854 of *Lecture Notes in Math.*, pages 372–401. Springer, Berlin-New York, 1981.
- [Sus] A. A. Suslin. Algebraic K -theory of fields. In *Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Berkeley, Calif., 1986)*, pages 222–244. Amer. Math. Soc., Providence, RI, 1987.
- [Yam] Go Yamashita. Bounds for the dimensions of p -adic multiple L -value spaces. *Doc. Math.*, (Extra volume: Andrei A. Suslin sixtieth birthday):687–723, 2010.
- [Zag] Don Zagier. Polylogarithms, Dedekind zeta functions and the algebraic K -theory of fields. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 391–430. Birkhäuser Boston, Boston, MA, 1991.